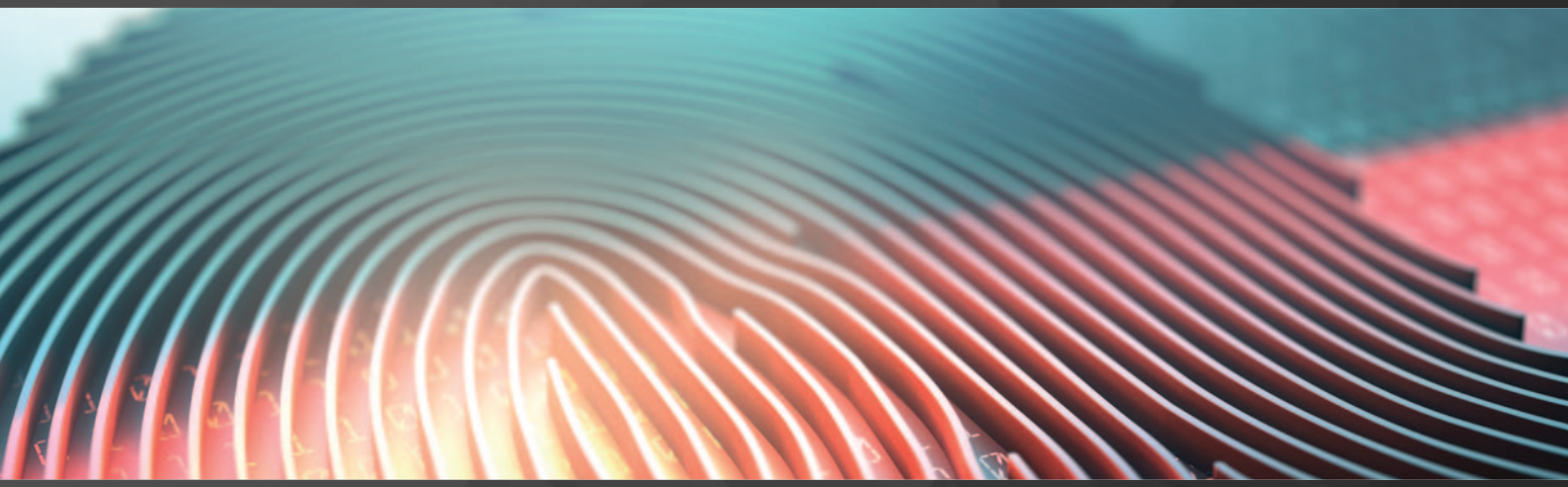
International Comparative Legal Guides



Cybersecurity 2020

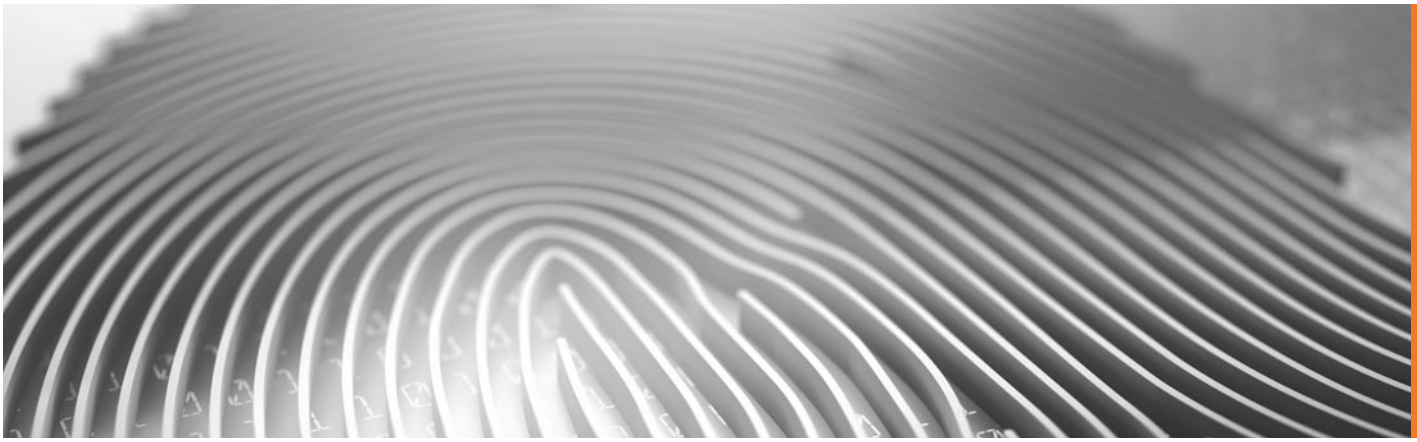
A practical cross-border insight into cybersecurity law

Third Edition

Featuring contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com



ISBN 978-1-83918-005-7
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Caroline Oakley
Rachel Williams

Deputy Editor
Hollie Parker

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

Cybersecurity 2020

Third Edition

Contributing Editors:
Nigel Parker and Alexandra Rendell
Allen & Overy LLP

Strategic Partners

Expert Chapters

Country Q&A Chapters

ICLG.com

From the Publisher

Dear Reader,

Welcome to the third edition of *The International Comparative Legal Guide to Cybersecurity*, published by Global Legal Group.

This publication, which is also available at www.iclg.com, provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world.

This year, there are three general chapters which provide an overview of key issues affecting cybersecurity, particularly from the perspective of a multi-jurisdictional transaction.

The question and answer chapters, which cover 32 jurisdictions in this edition, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, to whom the editors and publishers are extremely grateful for their invaluable contributions.

Global Legal Group would also like to extend special thanks to contributing editors Nigel Parker and Alexandra Rendell of Allen & Overy LLP for their leadership, support and expertise in bringing this project to fruition.

Rory Smith
Group Publisher
Global Legal Group

Effective Cyber Diligence – The Importance of Getting it Right


Nigel Parker


Alexandra Rendell

Allen & Overy LLP

Data is a valuable asset. Companies are increasingly seeking to acquire or merge with data-rich targets as a means to grow and enhance their business and keep pace with the fast-evolving digital environment. However, with the exponential growth of data in our connected lives comes the increased range and risk of cyber threats. Companies must carefully consider cyber risks in any M&A activity they may look to undertake so that they can balance both privacy and data security concerns and risks to their businesses, their investors and their customers, but also to safeguard against unintended consequences that may result from pursuing a target without undertaking sufficient due diligence.

Cyber-crime is estimated to cost the UK £27 billion a year, and the average cost to a large organisation of a data security breach is between £1.46 million and £3.14 million. A serious cybersecurity breach can also have a serious effect on a company's share price; for example, AOL, eBay and TalkTalk saw drops of 23.56%, 7.35% and 14.55% in the month after the announcement of a breach, respectively.

Cybersecurity Incidents may also result in wider losses, including:

- regulatory fines;
- business interruption;
- internal costs, including loss of management time and potentially significant costs incurred in remedying the Incident;
- damages in civil actions; and
- reputational damage and a loss of goodwill.

A cybersecurity Incident may also impact the integrity of the data or intellectual property in an organisation (for example, if information is stolen or deleted). Each of these will clearly have some impact, whether short or long term, on the value of a business. Taking measures to mitigate these risks, including undertaking effective cyber diligence, will therefore be of significant interest to any potential purchaser of a business.

What Do We Mean by Cyber Diligence?

Cyber diligence will be most effective when it is tailored to the business and transaction in question, so it essential to consider the scope of any diligence required at the outset. In some cases, high-level enquiry may be sufficient. However, in others, a more detailed examination will be required, and in some cases it may be beneficial to enlist the help of specialist technical experts.

Effective cyber diligence requires considering a number of questions to help scope the risks and the nature of the diligence required.

- **Is it a high-risk target?** Does the target regularly handle data that would make it attractive to a hacker? For example, does it operate in a sector that may increase its risk, such as the medical or healthcare sector, or defence and security? Does the target have a lot of valuable intellectual property that may increase its risk? Does the target operate in a high-risk jurisdiction?
- **Is the purchaser under an obligation to conduct due diligence?** Regulators in certain sectors are starting to request cyber diligence from entities they oversee. For example, the New York State Department of Financial Services enacted a regulation setting out cybersecurity requirements for financial services companies, under which the NYDFS has made clear it expects covered entities to have "a serious due diligence process, and cybersecurity should be a priority when considering any new acquisitions".[1] Any purchaser that is subject to specific regulatory requirements will need to ensure that the level of diligence conducted will meet regulatory expectations, as well as acting to mitigate commercial risks to the company.
- **What sort of data does the target handle?** Does the target regularly handle large amounts or personal data, or sensitive data? Is the target business primarily focused on processing consumer data, rather than business-to-business transactions? If so, it will be particularly important to consider data security and data protection compliance and processes.
- **What effect would loss of data have on the target?** In other words, how valuable is the relevant data to the business?
- **What data security systems and processes does the target have in place?** Cyber diligence should always involve an assessment of technical systems and governance policies and processes around data security, including business continuity and recovery plans. The scope and detail of this assessment will be informed by the cyber risk facing the target.
- **Does the target have a history of cyber attacks and data breaches?** Not all cyber Incidents must be reported under applicable laws, and many will not be. However, the target may keep an internal log of lower-level Incidents that were remedied without the need for any public statement, and so an early review of this (or asking early questions of management) will help inform the scope of further diligence that may be required.

What Might Effective Cyber Diligence Involve?

A cyber diligence process may involve a number of different activities, depending on the cyber risks identified for the target and the scope of the diligence that has been agreed. Each may uncover a variety of technical, legal and financial risks to the target business that a purchaser can consider in its overall assessment of the proposed acquisition. An effective cyber diligence process will also typically involve input from multiple teams, including legal advisors, technical advisors, day-to-day business teams responsible for managing the relevant data, and senior management.

- **Assessment of information assets:** It is essential to understand the nature of the data assets of the target. An assessment of these assets should cover: the value of the assets to the target; how and where they are held (for example, in the cloud, on proprietary servers, etc.); and contractual terms governing those assets, including in relation to transfer and security.
- **Security audits and risk assessments:** As a starting point, the purchaser may wish to use its own risk assessments and security audits as a guide to the principal issues to consider for diligence

of the target. If the target has a mature cybersecurity policy, it may also be able to provide copies of its own security audits for review. If, however, the target has never conducted its own security audit, or previous security audits have only been conducted by internal teams, the purchaser may wish to consider instructing its own advisors to conduct an audit. Studies have shown that security issues are more typically discovered by external third parties (such as auditors, security vendors or law enforcement agencies) than by internal teams. However, if the target agrees to an independent audit as part of the diligence process, a well-advised target may wish to commission its own report and then share this with the purchaser so as to retain as much control over the process as possible.

- **Regulatory compliance:** Assess the target's compliance with all relevant legal and regulatory standards in the jurisdictions in which it operates. This can involve public searches to confirm appropriate registrations have been made where required, a technical review of the security of the target's information assets, and a review of the policies and procedures that the target has in place to monitor security and report on it where necessary. A policy review should not only capture whether the relevant policies are in place, but also the extent to which those policies are implemented and monitored in practice (for example through internal audits or staff training programmes).
- **Historic breaches and recovery plans:** The purchaser should assess the target's history of data security breaches and how they were addressed. This assessment should cover:
  - the nature of the breaches (for example, whether triggered by internal or external factors);
  - the effect of the breaches on the target (including economic loss, business interruption and wider issues such as reputational damage);
  - how the target responded to those breaches; for example,: how quickly was the breach discovered? Was an Incident response procedure triggered, and if so what level of reporting took place? What remedial measures did the target put in place?; and
  - what, if any, steps did the target take following the breach to prevent reoccurrence?
- **Third party risk:** Consider the target's data sharing practices and arrangements with third parties, particularly if there are any third parties the target relies on to process, hold or otherwise manage its information assets. Review the contracts in place between the target and those third parties and consider how they may affect the target's risk. For example, does the third party have clear reporting obligations in the event of an Incident? Does the target have appropriate contractual protection (such as indemnities) if the third party breaches its obligations? The purchaser should also enquire as to what diligence the target did on the third party before, or during, the contractual relationship – has the target conducted any security audits on the third party to check how the third party protects information assets?
- **Employee risk:** Consider the target's internal policies and processes and how the target ensures that employees and senior management understand the cybersecurity risks facing the business and how to mitigate them. This may include an assessment of the target's internal governance structure for cybersecurity matters to understand who has day-to-day oversight of compliance. It will also typically include a review of the target's internal education and training programmes, internal compliance assessments and the nature and extent of cybersecurity information reported to the board.

Considering these issues as part of an effective cyber diligence process will not only help provide a more detailed insight into the target's network and technology risk profile before a merger or acquisition, but can also be used post-acquisition to help shape integration planning.

Case Study – Yahoo

In December 2014, Yahoo (now known as Altaba) suffered a massive breach of its user database resulting in the theft of hundreds of millions of its users' data. Yahoo discovered the breach within days, and Yahoo's Chief Information Security Officer notified the senior management and legal teams. However, Yahoo did not publicly disclose the breach until 2016 – in connection with an acquisition by Verizon Communications. In the intervening period, Yahoo had both failed to disclose the breach in its risk factor disclosures in annual and quarterly reports and in the due diligence process with Verizon. In total, all of Yahoo's three billion users were likely to be compromised.

The SEC found that Yahoo violated various provisions of the US Securities Act and the US Exchange Act in respect of market disclosures and misleading investors, and imposed a fine of $35 million – the SEC's first ever against a public company for failure to disclose a cyber breach.[2]

The other key consequence for Yahoo was the impact on the Verizon deal. Prior to the disclosure of the data breaches the parties agreed a purchase price of $4.8 billion. Following the disclosures, completion of the deal was delayed while the parties worked through the impact, eventually agreeing a revised price of $4.48 billion – a discount of $350 million. In addition, the two companies agreed to share legal and regulatory liabilities. While $350 million may seem like a heavy price to pay for Yahoo, it was rumoured at the time that Verizon was looking for a discount of $1 billion on the agreed purchase price.

Case Study – Marriott

A more recent example of unintended consequences following an M&A transaction, which again helps to highlight the importance of cybersecurity due diligence, is the UK Information Commissioner's (**ICO**) recent announcement of an intention to fine Marriott International, Inc. over £99 million for GDPR infringements following a data breach that was notified to the ICO in November 2018.

A variety of personal data contained in approximately 339 million guest records globally were exposed by the Incident, including some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (**SPG**) account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiry dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). Around 30 million guest records related to residents of 31 countries in the European Economic Area (**EEA**), and 7 million related to UK residents.

The Incident related to systems of the Starwood hotels group, and in particular the Starwood guest reservation database, which are believed to have been compromised in 2014. Marriott subsequently acquired Starwood in 2016 in a $13.3 billion takeover.

At the time of writing, the ICO has only published its intention to impose a fine, and so the ICO's public statements on the matter are comparatively brief. The ICO will consider any further representations by Marriott and will not publish any final enforcement notice, which would contain further detail of the relevant breaches and the basis for the ICO's decision to impose a fine, until the ICO has made its final decision. However, it is worth noting that in the ICO's statement,[3] the ICO drew particular attention to purported due diligence failings by Marriott in relation to the 2016 Starwood acquisition, saying "[t]he ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems". It remains to be seen what further conclusions the ICO will draw as to the impact a lack of sufficient cybersecurity due diligence had in this case.

Endnotes

1. https://www.dfs.ny.gov/industry_guidance/cyber_faqs.
2. https://www.sec.gov/litigation/admin/2018/33-10485.pdf.
3. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Alexandra Rendell is a senior associate specialising in commercial contracts, data protection, intellectual property and information technology law. Alexandra advises on complex commercial arrangements for a range of clients in the technology, life sciences and financial services sector, including outsourcing and service provision arrangements, licensing and IP/data exploitation.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 2639
Email: alexandra.rendell@allenovery.com
URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 15 partners with diverse backgrounds in data protection, bank regulation, anti-trust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

Franchising in a Sea of Data and a Tempest of Legal Change


Paul Luehr


Huw Beverley-Smith


Nick Rotchadl


Brian Schnell

Faegre Baker Daniels

I Introduction – So Much Data, So Many Laws

Franchisors and franchisees understand the value of data. Used properly, digital information flowing through computers and smartphones can improve the efficiency of operations, the effectiveness of marketing, and service to customers. What makes franchising unique is that franchisors and franchisees are independent businesses with different rights and responsibilities over the same customer data. The franchisor typically owns customer relationships based on a widely recognised brand and loyalty to a system built over time, while the franchisee typically serves the same customer through an independent business built on the franchisor's trademarks, as well as exceptional local service. Both the franchisor and franchisee may need access to personal information about the customer to satisfy their respective roles in a franchise system. At the same time, however, both now need to adapt to the California Consumer Privacy Act ("CCPA"), the European Union's General Data Protection Regulation ("GDPR") and other emerging privacy and data security laws that more aggressively protect personal information.

II Landscape of Emerging Privacy and Cybersecurity Laws for Franchising

1 The California Consumer Privacy Act ("CCPA") and Other State Laws

The CCPA is a sweeping privacy law that goes into effect January 1, 2020, and governs how businesses collect, share, and use consumers' "personal information", broadly defined as any information that "could reasonably be linked, directly or indirectly, with a particular consumer or household".[1] The CCPA gives consumers the right to ask businesses to disclose the specific items or categories of personal data they have collected, to delete that information, or stop sharing it with others. Businesses must update their websites and privacy policies, respond to consumer requests within 45 days, and potentially police data shared with third parties.

The CCPA's scope likely covers many franchisors and franchisees operating in the United States because it covers any for-profit entity "doing business in California" that collects personal consumer information and which: (i) has $25 million or more in annual gross revenues; (ii) alone, or in combination, buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices; or (iii) derives 50% or more of annual revenues from selling consumers' personal information.

Even franchisors and franchisees who believe they are not "doing business in California" may be surprised to learn that the CCPA applies to them. This is because the CCPA covers any entity that shares "common branding"[2] with another "business" and controls or is controlled by that business. A franchisor is likely subject to the CCPA if it has the "power to exercise a controlling influence over the management"[3] of a single California franchisee covered by the CCPA. At the same time, this type of "control" may pull non-California franchisees under the CCPA because they all operate in a common system.

While California and the CCPA currently have the attention of the business community, other state and federal laws cannot be overlooked. During the 2019 legislative sessions, at least 12 other states (Hawaii, Illinois, Maryland, Massachusetts, Minnesota, New Jersey, New Mexico, New York, Pennsylvania, Rhode Island, Texas, and Washington State) considered new privacy bills like the CCPA.[4] In addition, all 50 states require notification of data breach victims, and at least 25 U.S. states proactively require businesses to have "reasonable security procedures and practices" in place around personal data.[5] New York goes further and requires specific risk assessments, policies and procedures, penetration testing, vulnerability scans, audit trails, vendor screening, annual certifications, and 72-hour breach reporting for financial institutions.[6] The National Association of Insurance Commissioners ("NAIC") has proposed a similar Data Security Model Law for insurance companies,[7] and at least eight states have passed a version of the model law (Alabama, Connecticut, Delaware, Michigan, Mississippi, New Hampshire, Ohio, South Carolina).

At the federal level, franchise systems must still navigate a sector-by-sector approach to privacy law. For example, the Health Insurance Portability and Accountability Act ("HIPAA") governs personal information in health care records, the Family Educational Rights and Privacy Act ("FERPA") governs personal data in education records, and the Gramm-Leach-Bliley Act ("GLBA") governs personal information held by financial institutions.

2 The EU's General Data Protection Regulation ("GDPR") and Other International Laws

The European Union's GDPR went into effect in May 2018 and provided the roadmap for the CCPA and other new privacy laws around the globe. Under the GDPR, companies generally must:

- include specific information in privacy policies;
- maintain internal records of data processing activities;
- specify the legal basis for processing of personal data;
- obtain explicit consent, or have another appropriate legal basis under the GDPR, to process "special categories" of personal data including related to health, racial or ethnic origin, politics, religion, sexuality;
- disclose, delete, or stop processing personal data upon request from the data subject in certain circumstances;
- limit the processing of personal data to what is necessary and not retain personal data for longer than necessary for the specified processing purposes;

- carry out data protection impact assessments for new and innovative forms of processing which pose a "high risk" to individuals;
- require vendors to implement appropriate data protection safeguards;
- implement safeguards when transferring personal data to countries outside the EU;
- notify breaches to regulators within 72 hours; and
- in certain circumstances, appoint a data protection officer ("DPO").

Compared to the CCPA, the GDPR puts less onus on the consumer to protect his or her data. For example, companies must disclose their legal basis for processing personal data, the purposes of processing and details of third party recipients at the time of collection and generally document data activities internally, whether consumers ask about their information or not.

The GDPR has an expansive scope. It not only applies to organisations with an established presence in the EU, but also to organisations that offer goods or services to customers in the EU or that monitor their behaviour in the EU. The widened scope means many non-EU businesses will now be subject to European data privacy laws. For example, businesses that offer online services from outside the EU will likely be covered if they target customers in the EU, for example by offering goods or services in a local language or currency. Non-EU companies also will likely be covered if they monitor online activity or physical location (e.g., customer profiling through cookies or geo-location tracking).

Many countries have followed the GDPR model and passed comprehensive privacy statutes that cover their entire economies. In Brazil, for example, the *Lei Geral de Proteçao de Dados* ("LGPD") will take effect in 2020 and patterns itself after the GDPR in terms of statutory definitions, data subject rights, and even monetary penalties. Canada has updated its *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). While it is more focused on individual "consent", like the GDPR, the Canadian statute applies nationally and requires data minimisation, access rights, business accountability, and breach reporting. In Asia, Japan has amended its national Act on the Protection of Personal Information ("APPI"), established a new Personal Information Protection Commission ("PIPC"), and reached an agreement with the EU to recognise the "adequacy" of each other's privacy laws. Similar national data protection laws abound. As one Forrester consultant stated: "Although GDPR is just one year old, many nations have been inspired by the scope and depth when drafting their own privacy bills. It seems that every week news breaks that another jurisdiction is implementing personal data guidelines."[8]

III Potential Costs and Liability

While these new privacy and cybersecurity laws impose broad compliance duties on franchise systems, the effect of these laws is compounded by the daily onslaught of data breaches. A data breach can cost millions of dollars, and liability for a breach can spread across both franchisors and franchisees.

1 The Cost of Data Breaches

The average data breach costs $3.92 million according to a 2019 global survey conducted by the Ponemon Institute and sponsored by IBM. In the U.S., the cost is a whopping $8.19 million.[9] These figures represent an average compromise of about 26,000 individual records (about one spreadsheet worth of data) and do not include "mega breaches" like Equifax that involve millions of victims and even higher costs. The IBM/Ponemon report shows that the healthcare industry incurs the largest losses from data breaches, but no industry is immune. In fact, the odds of experiencing a breach within the next two years are 29.6% across all companies. Moreover, the damage from a data breach can linger, with 33% of the costs coming more than a year after discovery of an incident.[10]

2 Direct Liability

Both franchisors and franchisees may be *directly liable* for these costs, depending on where hackers hit a system. Under the CCPA, if unencrypted, sensitive personal information like social security numbers are acquired without authorisation and the business failed to implement a reasonable security programme, then consumers may bring individual or class actions after a 30-day period to "cure" any harm.[11] Among other relief, the CCPA allows statutory damages of $100 to $750 per consumer per incident OR actual damages, whichever is greater. Additionally, the California Attorney General ("AG") may bring action for an injunction and civil penalties up to $2,500 per violation, or up to $7,500 for each intentional violation. It remains to be seen if private litigants and the AG will move aggressively under the CCPA; however, history does not bode well. Under the Telephone Consumer Protection Act ("TCPA"), a privacy law focused on unwanted text messages and robocalls, franchisors have entered multi-million-dollar settlements when faced with similar class action rights and fixed damages per incident.[12]

GDPR fines for non-compliance are potentially vast – up to 4% of total worldwide annual turnover (i.e. revenues) of a company (or potentially a company group) or €20,000,000, whichever is higher. The potential fines apply to many of the core provisions of the GDPR, including the six general principles of processing. A lower tier of fines – up to €10,000,000 or 2% of total worldwide annual turnover – applies to a failure to appoint a Data Protection Officer, implement appropriate technical and organisational security measures, maintain written records, or report a data breach. These fines do not necessarily bear any relation to the actual harm caused to a data subject, and national data protection authorities ("DPAs") can also require corrective measures, impose temporary or permanent bans on processing, or suspend international transfers of data.

A franchisor has already been hit with one of the largest fines under the GDPR to date. On July 9, 2019, the UK's Information Commissioner's Office (the "ICO") announced its intention to fine Marriott International, Inc. £99,200,396 for GDPR violations.[13] The proposed fine arises from an old cyber-attack on the reservation system of Starwood properties, a collection of brands that Marriott acquired in 2016. According to the ICO, "a variety of personal data contained in approximately 339 million guest records globally were exposed by the incident".[14] So far, the ICO has not sought to impose direct liability against Marriott franchisees or addressed whether any franchisees may bear some cost for the data breach.

3 Vicarious Liability

Apart from direct liability, a franchisor can also find itself responsible for the wrongdoing of its franchisee(s) under a theory of "vicarious liability". Privacy and cybersecurity are like many other franchising issues because a franchisor must balance: i) the franchisor's desire to impose data controls that protect the brand; and ii) its franchisees' status as independent businesses with day-to-day control over operations. Depending on the jurisdiction and applicable law, franchisors who exercise too much control over privacy and cybersecurity may face claims of vicarious liability. Two cases illustrate this point.

a. *FTC v. Wyndham Worldwide Corp.*

In *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D. N.J. Apr. 7, 2014), *aff'd* 799 F.3d 236 (3rd Cir. Aug. 24, 2015), the Federal Trade Commission ("FTC") brought action under Section 5(a) of the FTC Act against several Wyndham entities. The FTC pointed to a previous privacy policy on the website for Wyndham Hotels and Resorts, LLC ("Wyndham Hotels and Resorts") and alleged that the franchisor had deceived consumers and misrepresented that it had implemented reasonable and appropriate measures to protect personal information. 10 F. Supp. at 607, 626.

Wyndham Hotels and Resorts sought to dismiss the FTC's action by arguing that Wyndham-branded hotels were "legally separate entities that each maintain their own computer networks and engage in their own data-collection practices". *FTC v. Wyndham*, 10 F. Supp. 3d at 627. It explained that the privacy policy on its website "specifically excludes the Wyndham-branded hotels from the policy's data-security representations and that such exclusion of responsibility over franchisees' actions is consistent with franchise law". *Id.* The FTC countered that Wyndham Hotels and Resorts was responsible for any data-security failures by "permit[ing] computers with unreasonable data security measures on its network". The FTC also claimed it was unnecessary to allege separately that Wyndham controlled franchisees' security practices because the data security failures were attributable to Wyndham Hotels and Resorts itself. Finally, the FTC claimed that Wyndham Hotels and Resorts in fact had control over the relevant aspects of the franchisees' data security practices. *Id.*

The district court considered these arguments and rejected a motion to dismiss by franchisor Wyndham Hotels and Resorts. The court relied on the FTC's allegations that Wyndham Hotels and Resorts failed to: i) adequately inventory computers connected to its network in order to manage the devices; ii) employ reasonable measures to detect and prevent unauthorised access to the defendants' computer network; iii) conduct security investigations; and iv) follow proper incident response procedures, including failure to monitor the network for malware used in a previous intrusion. *Id* at 629. As a matter of law, the district court also rejected the argument that Wyndham Hotels and Resorts was a separate entity from Wyndham branded hotels, or that the privacy policy properly disclaimed data security practices at Wyndham branded hotels. *Id.* at 629–630. The district court explained that a "reasonable customer would have understood that the policy makes statements about data-security practices at Hotels and Resorts and Wyndham-branded hotels, to the extent that Hotels and Resorts controls personally identifiable information". *Id.* at 630.

Wyndham Hotels and Resorts eventually settled with the FTC.[15] The settlement acknowledged that a "Wyndham-branded hotel" is "an independently-owned hotel that is operated in the United States pursuant to a management or franchise agreement", but the FTC still required the franchisor to maintain a security programme for 20 years, identify risks from Wyndham-branded hotels, design and implement reasonable safeguards to control risks at Wyndham-branded hotels, and certify whether the franchisor treated any network of a Wyndham-branded hotel as an untrusted network.[16]

b. *Peterson v. Aaron's, Inc.*

In another case, *Peterson v. Aaron's Inc.*, 108 F. Supp. 3d 1352 (N.D. Ga. June 4, 2015), a separate court found a franchisor liable alongside its franchisee because the franchisor provided tools to violate privacy obligations and learned of those privacy violations. This case focused on Aaron's, Inc. ("Aaron's"), a franchisor of businesses involved in the sale and leasing of personal computers. The plaintiffs alleged that an Aaron's franchisee installed software on computers to remotely access web camera photographs, user activity logs, and other private information stored on computers leased and purchased by the plaintiffs. 108 F. Supp. at 1354. The plaintiffs claimed that Aaron's was liable for common law invasion of privacy. *Id.* The plaintiffs admitted that Aaron's was not directly liable but claimed that Aaron's was liable for its franchisee's torts because Aaron's aided and abetted its franchisee's surveillance of customers. *Id.* at 1357.

The court denied Aaron's motion to dismiss. The court explained that plaintiffs adequately alleged that Aaron's knew its franchisee was invading its customers' privacy and provided substantial assistance to aid the franchisee's unlawful acts, including: i) promoting the offending computer program to the franchisee; ii) training the franchisee's personnel on how to use the offending program; iii) granting its franchisee access to a portal on Aaron's intranet by which the franchisee illegally spied on customers; and iv) providing its franchisee with advice about how to avoid conflicts between the offending program and antivirus software. *Id.* at 1357. The court also found that plaintiffs had adequately alleged that Aaron's employees knew the franchisee had used the offending program to conduct key-logging and take photographs of customers via the web camera. *Id.* Ultimately, the court concluded that Aaron's could be held jointly liable for invasion of privacy claim under Georgia law, which recognises that "persons acting in concert under [certain] situations may be liable for the acts of others". *Id.* at 1357–1358.

4 Brand Damage

Even though it is an intangible asset, the franchisor's trademarked brand is perhaps the most important asset of any franchisor and the franchise system, and the damage caused by privacy violations and/or data breach can be a major setback for a franchise system. Customers will likely punish the entire franchise system for a perceived violation, without distinguishing between the franchisor and multiple franchisees. Franchisees may encounter lower sales due to the wrongdoing of a franchisee hundreds of miles away, while the franchisor may encounter lower percentage-based royalties across all locations. The franchisor's sales of franchise units to quality business owners also may suffer for months or years to come.

The potential damage to a brand is not just hypothetical. In its 2019 study, the Ponemon Institute found that out-of-pocket expenses for legal fees, forensic experts, ID theft protection, victim notification, fines and litigation accounted for less than half of all breach costs. Most losses from data breaches stem from *indirect costs* like business down time, redirected IT resources, customer turnover, tarnished reputation, and lost goodwill. In the study, lost business by itself accounted for 36% of all breach costs.[17]

IV Practical Actions for Franchisors to Take on Privacy and Data Security

The challenge of sharing sensitive data while complying with emerging privacy and data security laws may appear overwhelming at first. Franchise systems, however, can take actionable steps to improve their business and lower their risk. This section covers actions that franchisors can take right now to have a meaningful impact on privacy and data security.

1 Map Data and Records Processing Activity

Data mapping is an important first step toward protecting personal information. Companies cannot protect what they do not know they have. Data mapping tracks how personal information flows through a franchise system. A good data map identifies what personal information is collected, when it is collected, when it is transferred, when it is deleted, where and how it is processed and retained, the business purpose for collecting and sharing it, from whom it is collected, and to whom it is transferred. Data mapping allows companies to meet requirements like the GDPR's requirement to maintain records of data processing, and data mapping lies at the core of every industry standard that describes "reasonable" cybersecurity.[18] In addition, data mapping allows an attorney to offer sound advice, especially in the heat of a data breach investigation when speed and accuracy matter most.

Data mapping does not stop at the franchisor's four walls. Franchisors should consider verifying the practices of third parties who share or transfer personal information with the franchisor. This is particularly true for franchisees who handle consumer data that belongs to the franchisor under the terms of the franchise agreement. To help with data mapping and other privacy compliance obligations, franchisors may consider including provisions in the franchise agreements that require franchisees to cooperate with requests about personal information of consumers. Franchisors may also provide

guidelines and recommendations about how franchisees can conduct their own data mapping.

2 Revise Internal Policies and Procedures

Franchisors should also update both internal privacy and cybersecurity policies and procedures. On the privacy side, franchisors should make sure that they have a privacy statement that aligns with the company's philosophy and employee handbook. If the franchisor monitors employees' web activity or communications or screens applicants and performs background checks, more specific documents may need to be prepared, especially in Europe where employees have broad rights to privacy even in the workplace and employers will need to rely on a legal basis other than the employees' consent. Franchisors also should consider implementing a process for a "privacy impact assessment" ("PIA"), also called a "data protection impact assessment" ("DPIA") under GDPR requirements. A PIA describes the procedure that companies should follow before collecting new pieces of personal information or processing current personal data in new ways, for example, for new marketing activities or products. A PIA generally includes documentation that describes the new data or process and an approval process to be followed by managers or a larger privacy team.

On the cybersecurity side, the franchisor should make sure that it has a set of written policies and procedures that aligns with applicable laws and industry standards like the Payment Card Industry Data Security Standards ("PCI DSS") or the International Standards Organization 27001-2 standard for information security management ("ISO 27001-2"). Drafting or updating cybersecurity policies and procedures can be time-consuming because a dozen or more topics should be covered (e.g. data classification, asset management, encryption, passwords and access controls, network scanning and patching, annual assessments); however, most courts will likely require this type of documentation to find that a franchisor has implemented a "reasonable" security program under the GDPR, CCPA, or other laws.

Franchisees should have their own privacy and cybersecurity policies and procedures, but each franchisor must decide how much control they should exercise. A franchisor that mandates a particular privacy or cybersecurity policy for franchisees should understand the risk of vicarious liability if those franchisees mishandle data, yet some franchisors may decide it is a worthy trade-off given the potential damage from a data breach or privacy violation. Other franchisors may want to exert less control by merely recommending draft policies without mandating the final terms.

3 Create an Incident Response Plan

Perhaps the most important document in any set of cybersecurity policies is an incident response ("IR") plan. This plan should facilitate a quick and effective response to a potential data breach. A good plan starts with a good team, and the IR team should extend well beyond the IT department and include Legal, HR, Communications, Audit/Risk, and Operations. The plan also should clearly define where employees should report a potential breach (usually the Help Desk), how IT staff should quickly assess possible threats, escalate a real threat to the full IR team and eventually to the CEO and the Board. The plan should provide clear direction about preservation of forensic evidence, possible containment efforts, and communication protocols. In-house or outside counsel usually should lead the overall breach investigation because so many implicit questions are legal in nature: What type of data was accessed or taken? Does the compromise trigger a notification obligation? If so, by whom (e.g. the franchisee *and* the franchisor), to whom, and how fast? No franchisor should try to respond to a large potential breach by itself because there are many experts who do this for a living. Therefore, the IR plan should include a hot sheet with the mobile numbers and emails of outside breach counsel, forensic experts, insurance representatives, public relations experts, notification and credit monitoring firms, and law enforcement officers. Franchisors should also consider carefully when they should send a communication to all franchisees and when an investigation should remain confidential.

4 Manage Third Parties with Personal Information

Another important aspect of both privacy and cybersecurity is vendor management. Franchisors contract with many outside vendors and should consider amending their contracts to require a service provider to:

- delete a consumer's personal information upon the company's request;
- not use any of consumer's personal information except to perform the services;
- not retain, use or disclose any of consumer's personal information except to perform the services;
- not discriminate against a consumer who has exercised his or her privacy rights (including by providing a different level of service, denying goods or services); and
- certify that the service provider understands and will comply with these prohibitions, as required under the CCPA.

If a franchisor is considering the purchase of another franchise system, similar third-party risk issues can arise. While this article does not cover the full cyber due diligence that should go into M&A deals, the franchisor should at least seek full copies of any assessments, audits, or certifications that the acquisition target may possess related to privacy and data security.

5 Revise Websites and Marketing

Looking outward, franchisors should consider updating their websites in response to the CCPA, GDPR and other privacy laws. Under the CCPA, a business must provide a California-specific disclosure that describes: the consumers' rights under California law; the categories of personal information it has collected about consumers in the preceding 12 months; whether personal information has been sold or disclosed for a business purpose in the past 12 months; and what categories (if any) have been sold or disclosed. The GDPR similarly requires an accessible, plain-language privacy policy that describes specific categories of personal information, the purpose and legal basis for processing that information, and the right to access or request deletion of the personal information. The CCPA goes a step further: if the business sells personal information, it must put a clear and conspicuous link on its homepage, titled "Do Not Sell My Personal Information". As an alternative to this homepage link, the business can direct California consumers to their own dedicated disclosure page.

6 Create a Consumer Rights Response Plan

Both the CCPA and the GDPR will require franchisors to respond quickly to the requests described above. Under the CCPA, for example, franchisors generally must provide information free of charge and deliver it within 45 days of receiving a verifiable request. Under the GDPR, the response time limit is 30 days, subject to extensions in certain circumstances. Therefore, franchisors will need to have tools, procedures, and response templates in place to meet these deadlines. Several complicating issues will likely plague all franchise systems: Who will collect, coordinate and track the information about a consumer who has visited multiple franchise locations in a single year (e.g. for an ice cream or a haircut)? Who needs to respond when a consumer submits a request to a local franchisee – just the local franchisee, or the franchisor on behalf of the whole system?

7 Conduct Training and Testing

The foregoing tips will mean little if a franchisor adopts them all in theory but never puts them into practice. To make meaningful progress toward better privacy and cybersecurity, franchisors must train their staff when they are hired, then again at least annually, and ideally on a continuous basis using intranets, email alerts, and other technology. Some key areas of training should include:

- the franchisor's commitment to privacy and cybersecurity and the need to retain customer trust;
- the types of data that need extra care and protection (e.g. government ID numbers, financial and health data, usernames and passwords);
- procedures to respond to consumer data requests;
- procedures to report a potential data breach; and
- common email attacks, where many breaches begin.[19]

Franchisors also would be wise to annually test their IR plan through table-top exercises or cybersecurity "war games". In fact, the Ponemon Institute found that, if an organisation extensively tested its IR plan, it could save $1.23 million during an actual breach, compared to those organisations that did not have a plan or test it.[20]

8 Revise Franchise Agreements

Finally, franchisors need the cooperation of their franchisees to comply with emerging privacy and data security laws. Franchisors also need to clearly delineate franchisees' own obligations related to customer data that they share. The franchise agreement is an appropriate place to do this, although some of the key points also might be appropriate to include in the franchisor's operations manual. Subject to each franchisor's willingness to retain and/or exercise control over certain aspects of a franchisee's business, which may likely increase the vicarious liability risk, franchisors may want to consider the following:

- Clarify that each franchisee is responsible for its own compliance with any applicable privacy and data security law, including, but not limited to, the CCPA and GDPR.
- Require the franchisee's cooperation in any franchisor review or assessment of the franchisee's privacy and data security practices.
- Require the franchisee's cooperation to respond to consumer or data subject requests under any applicable privacy and data security law, including, but not limited to, the CCPA and GDPR.
- Prohibit the franchisee from selling or transferring any of a consumer's personal information except to perform its obligations under the franchise agreement.
- Prohibit the franchisee from retaining, using or disclosing any of a consumer's personal information except to perform its obligations under the franchise agreement.
- Require the franchisee to have a privacy policy, with an express term that it does not and is not intended to in any way inhibit the franchisor from carrying out the franchisor's own privacy and cybersecurity obligations.
- Require the franchisee to immediately notify the franchisor of any suspected data breach.
- Require the franchisee to annually provide the franchisor with a copy of an applicable privacy or cybersecurity assessment or certification (e.g. PCI DSS, ISO 27001, or AICPA SOC2 certification).
- Require the franchisee to obtain specified types of cybersecurity insurance coverage with the franchisor named as an additional insured.

9 Conclusion – Time to Jump In

Neither the need for new technology and data, nor concerns about privacy and cybersecurity, will disappear in the near future. Franchisors and franchisees will continue to collect, analyse, and share digital information in order to satisfy customer needs and improve operations. At the same time, however, a wave of new privacy and cybersecurity regulations will continue to wash over the franchise industry. Franchisors who ignore their compliance obligations will likely drown in privacy litigation, data breaches, and lost business. Therefore, franchisors would be wise to adapt, track their data, update their policies and procedures, train staff, and revise their franchise agreements to reflect new privacy and cybersecurity duties. In short, it is time to jump in and swim with the current.

Endnotes

1. The CCPA explains that "personal information" may include an individual's name, alias, postal address, unique personal identifier, IP address, email address, account name, social security number, driver's licence number, passport number or other similar identifiers, as well as biometric information, history of purchasing products or property, browsing history, search history, geolocation data, audio, electronic, visual, thermal, olfactory or similar information, education, and employment or professional information. The CCPA is not limited to digital information collected online. It applies to the collection and sale of all personal information collected by a business from consumers.
2. The CCPA defines "common branding" to mean a shared name, service mark, or trademark.
3. The California Supreme Court has previously found that a franchisor may exercise "control" over franchisees without creating an agency relationship with their independent contractor franchisees in the case, *Patterson v. Domino's Pizza, LLC*, 60 Cal. 4th 474 (2014).
4. M. Noordyke, "US State Comprehensive Privacy Law Comparison", Int'l Ass'n of Privacy Prof'ls (IAPP) Resource Center *available at* https://iapp.org/resources/article/state-comparison-table/.
5. Nat'l Conf of State Legislatures (NCSL), "Data Security Laws | Private Sector", *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.
6. 23 NYCRR 500, *available at* https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.
7. *See* NAIC, "Data, Innovation & Cyber", *available at* https://www.naic.org/cipr_topics/topic_cyber_risk.htm.
8. E. Iannopollo, "It's Here: The 2019 Forrester Global Map Of Privacy Rights And Regulations", *available at* https://go.forrester.com/blogs/its-here-the-2019-forrester-global-map-of-privacy-rights-and-regulations/.
9. *See* Ponemon Institute & IBM, Cost of a Data Breach Report 2019, *available at* https://newsroom.im.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years.
10. *Id.*
11. Consumers cannot bring a private right of action for the loss of broadly defined "personal data" under the CCPA. Instead, a consumer can only bring a private right of action if there is unauthorised acquisition of more sensitive data defined by the state's data breach notification law at Civ. Code § 1798.81.5 (d)(1)(A).

12. *See* Scott Flaherty, Papa John's Will Deliver $16.5M To End TCPA Claims, Law 360, *available at* https://www.law360.com/articles/442855/papa-john-s-will-deliver-16-5m-to-end-tcpa-claims.
13. Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, *available at* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.
14. *Id.*15. Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk, *available at* https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.
16. Stipulated Order for Injunction, Case No. 2:13-CV-01887-ES-JAD (D. N.J. Dec. 9, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/151209wyndhamstipulated.pdf.
17. Ponemon Institute & IBM, Cost of a Data Breach Report 2019, at 34.
18. Industry standards like the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF") often fold data mapping into their "Data Classification" or "Asset Management" requirements.
19. According to the 2019 Verizon Data Breach Investigations Report ("DBIR"), 94% of all malicious software found in cyber attacks is delivered via email. 2019 Verizon Data Breach Investigations Report (DBIR) 13, *available at* https://enterprise.verizon.com/resources/reports/dbir/2019/.
20. Ponemon Institute & IBM, Cost of a Data Breach Report 2019 at 9.

Paul Luehr partners with clients to optimise their privacy and cybersecurity practices, from risk management to incident response. As the leader of the firm's privacy and cybersecurity team, Paul understands that cybersecurity crises can be profoundly costly, and they can strike organisations across a wide range of industries. Drawing from 25 years on the cutting edge of data privacy and cybersecurity, Paul helps clients avoid becoming a cautionary tale. He has led investigations into several of the top data breaches on record. Paul has overseen forensic teams on data incidents affecting national retailers, financial institutions, hospitals and national health care companies, universities, hotel chains, defence contractors and online providers.

Faegre Baker Daniels
2200 Wells Fargo Center
90 S. Seventh Street
Minneapolis, MN 55402
USA

Tel: +1 612 766 7195
Email: paul.luehr@FaegreBD.com
URL: www.faegrebd.com

Huw Beverley-Smith advises customers and suppliers on a wide range of international transactions and regulatory issues, including technology, telecommunications and business process outsourcing, complex services agreements, intellectual property ownership and licensing. He counsels clients on privacy and cybersecurity issues and helps navigate regulatory hurdles and operational and commercial risks.

Faegre Baker Daniels
7 Pilgrim Street
London, EC4V 6lB
United Kingdom

Tel: +44 20 7450 4551
Email: huw.beverley-smith@FaegreBD.com
URL: www.faegrebd.com

Nick Rotchadl represents clients in commercial litigation and compliance matters, with an emphasis on franchise, distribution and software development matters. Nick represents franchisors in litigation, arbitration and mediation throughout the United States. He also advises franchisors on pre-litigation dispute resolution, the franchisor-franchisee relationship and compliance matters. He represents franchisors across industries that include restaurants, food and beverage, retail, leisure and fitness, health care, hospitality, and commercial and consumer services. Nick also helps businesses resolve and litigate disputes about software development and implementation projects. For these disputes, he helps clients investigate potential claims and defences, demand and negotiate resolution, and proceed through mediation, arbitration and/or litigation. He has experience navigating complex software disputes.

Faegre Baker Daniels
2200 Wells Fargo Center
90 S. Seventh Street
Minneapolis, MN 55402
USA

Tel: +1 612 766 6864
Email: nick.rotchadl@FaegreBD.com
URL: www.faegrebd.com

Brian Schnell leads FaegreBD's franchise and distribution practice and is widely recognised as a thought leader in franchising legal circles. He is passionate about franchising and has devoted more than 30 years to finding practical and often creative solutions for clients. He represents franchisors with headquarters based across the United States and abroad. Brian's experience includes serving as the COO and Chief Legal Officer during 2012 for one of the country's leading health care franchisors. With this unique legal and business background, Brian counsels both emerging and mature franchisors, ranging from companies with thousands of locations worldwide to companies in the initial stages of building franchise systems.

Faegre Baker Daniels
2200 Wells Fargo Center
90 S. Seventh Street
Minneapolis, MN 55402
USA

Tel: +1 612 766 7699
Email: brian.schnell@FaegreBD.com
URL: www.faegrebd.com

Why AI is the Future of Cybersecurity


Akira Matsuda


Hiroki Fujita

Iwata Godo

Overview Surrounding Cybersecurity

What is Cybersecurity?

Cybersecurity is defined as the "*preservation of confidentiality, integrity and availability of information in the Cyberspace*" in Article 4.20 of ISO/IEC 27032:2012.

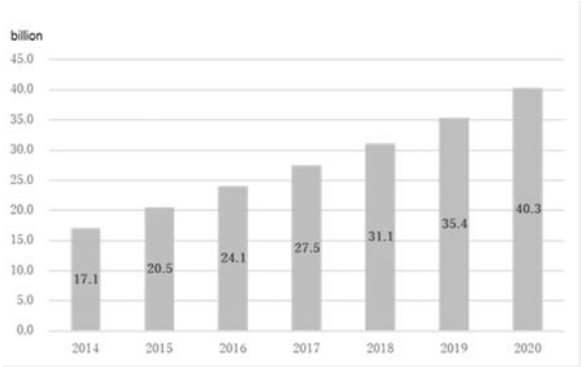
Furthermore, the cyberspace is defined as a "*complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*" in Article 4.21 of ISO/IEC 27032:2012.

Threats in cyberspace

As internet access becomes more pervasive across the world and IoT devices become increasingly common and cyberspace expands rapidly, the number of cyberattacks continues to grow. While an expanding cyberspace can be of great benefit to the public, the malicious use of cyberspace can result in significant economic and social losses. In cyberspace, cyber attackers have an asymmetric advantage over defenders. In particular, if defenders lag behind cyber attackers in terms of technology or defence systems, this advantage is likely to be enhanced. Unlike cyber attackers, it is difficult for defenders to introduce a new trial technology because the defenders' main role is to ensure the stability of the defence systems which could be potentially harmed and undermined by the new trial technology.

Expansion of cyberspace

Along with technological development, cyberspace keeps growing. For example, there were globally 27.5 billion IoT devices active in cyberspace in 2017, and it is estimated that this number will reach about 40 billion by 2020.[1]



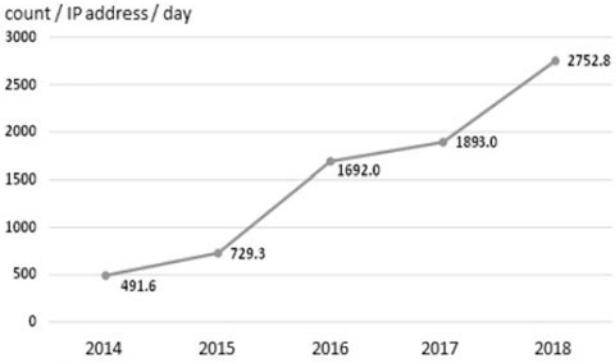
Note: The data is from "Cybersecurity 2019" by National center of Incident readiness and Strategy for Cybersecurity of Japan

The governments of many countries share the view that digitalisation is transforming every aspect of our economies and societies. The data is increasingly becoming an important source of economic growth, and its effective use should contribute to social well-being around the world. In order to facilitate this process, the "Osaka Track" framework aimed at promoting international policy discussions and the drafting of international rules to enable the free movement of data across borders (international rules on trade-related aspects of electronic commerce at the WTO) with Japan intending to be a key player, was launched on 28 June 2019.

Threats in cyberspace

As cyberspace keeps growing, the frequency of cyber attacks is increasing as a global trend. For example, in Japan, the number of unexpected connection attempts detected by the National Police Agency has risen to 2,752.8 per IP address per day in 2018.

Number of unexpected connection attempts detected by the National Police Agency of Japan



Note: From "Threats in Cyberspace 2018" by the National Police Agency of Japan.

New technologies and services, such as AI and IoT, could bring about substantial benefits to the society of the future as a society in which new values and services are created continuously, making people's lives more conformable and sustainable. On the other hand, there is a growing concern that these technologies could also be used in malicious ways. The risk is that users and providers of AI or IoT related services will not be able to sufficiently and adequately control these technological developments and their use. With the growth of cyberspace, new threats are emerging and also as to their scale, scope, and frequency and threats are escalating as more sophisticated and organised attackers are designing targeted attacks to damage or disrupt critical infrastructures and services. These disruptions can have a huge financial impact or paralyse vital activities. Cyberattacks can generally lead to loss of money, theft of

personal information/identity/IP, and damage to reputation and safety, cause problems with business services, transportation, health and power.

For example, the Central Bank of Bangladesh was hacked in December 2015, resulting in the embezzlement of about US$ 81 million, and a state-owned power company substation was attacked in December 2016 in Ukraine, resulting in a one-hour blackout. In Japan, cyber attacks have been successfully conducted to steal crypto assets in 2018.

Superiority of cyber attackers

Cyberspace is a place where everyone can utilise new information and communication technology without being constrained by location and time. A Cyber attacker has the decisive advantage as he can easily copy and disseminate data and information, including computer viruses/malware, and can flexibly use advanced technologies such as AI and blockchain. In contrast, it is generally difficult for defenders to respond to cyber attacks because the resources they can use are limited, no defensive capability remains indefinitely effective and they are forced to respond with their then currently existing systems and technologies to ensure the stability and resilience of their defence system. Unlike Cyber attackers, it is difficult for defenders to introduce a new trial technology because the new trial technology can harm or undermine the stability of defence systems. In addition, it is impossible to completely eliminate vulnerabilities caused by human errors linked to the use of information systems, so that many cyber attacks involve looking for weaknesses in user behaviour that can be exploited through seemingly legitimate means (so-called "social hacking/social engineering").

Countermeasures

As cyber attacks are spreading in Cyberspace, where attackers seem to have a constant decisive advantage over defenders and their ability to assess and address risks, "Active Cyber Defense" can be considered to be an effective countermeasure to such cyberattacks. Having an "Active Cyber Defense" means that the organisation proactively protects itself in advance rather than responding to a cyber attack which has occurred. In Japan, for example, the Ministry of Internal Affairs and Communications, which is the national watchdog in charge of cybersecurity-related laws and regulations, and the National Institute of Information and Communications Technology, which researches and promotes information and communications technology, have collaborated with internet service providers to launch the "NOTICE" program designed to investigate IoT devices which might be misused/hacked in cyber attacks because of weak authentification mechanisms (IDs and passwords), and to alert users. We understand that similar objectives are being pursued in many other countries.

To organise an "Active Cyber Defense", the utilisation of AI is considered to be very important. This is because Cyber attackers always use new offensive tools to conduct cyber attacks, so that, in order to respond to cyber attacks effectively, detection and analysis by AI are necessary. AI technology can be used to track new patterns or offensive strategies which could otherwise not be detected without machine learning mechanisms. In addition, by introducing AI in their defence strategy, humans can focus on their analysis of causes and impact at the time of a cyber attack and as the case may be react to false detection. It is possible to increase the efficiency and accuracy of defence systems in cyberspace but to stay one step ahead is challenging.

Relationships Between Cybersecurity and AI

Trends/directions followed by AI utilisation

As for the direction of AI utilisation, as a general principle, there is a common understanding that it is extremely important not to excessively rely on AI and that humans should keep some control over the use of AI and AI-generated results and output. Ethics and morality would be negatively impacted by the excessive use of, and total dependence on, the use of AI. At this stage, many governments or integrated areas want to provide directions and guidance for the use of AI by issuing guidelines. For example, the "Principles for a Human-centric AI Society" were published in March 2019 in Japan and "Ethics Guidelines for Trustworthy AI" was published by the European Commission in April 2019.

Relationship between Cybersecurity and AI

The globally accepted and prevalent categorisation of the relationships between Cybersecurity and AI is the following and can be divided into four categories: "Attacks using AI"; "Autonomous attacks by AI"; "Attacks against AI"; and "Security measures using AI".

Attacks using AI

Cyber attackers use AI for cyber attacks. Such attacks are actually occurring in the real world.

Autonomous attacks by AI

AI performs cyber attacks autonomously without human intervention. However, under the current AI model, this category is not yet in existence. Once it becomes technically possible for AI to perform cyber attacks autonomously without human intervention, one difficulty will be to allocate responsibility as regards civil damages caused by cyber attacks.

Attacks against AI

This category covers cyber attacks against AI and the so-called "Adversarial Learning"; for example, where a cyber attacker may feed fake data to AI. Such an attack could become realistic in the future if human involvement in AI monitoring declines and the use of AI for critical decisions (such as diagnostics and investment decisions, etc.) becomes general.

Security measures using AI

This category covers defenders using AI against cyber attacks. Various attempts have already been made, such as the automation of malware detection. At present, human beings continue to be responsible for determining those issues to be solved by AI and interpreting decisions by AI. Therefore, it is necessary to develop human resources that can fully utilise AI.

We will discuss "Security measures using AI" further in detail below.

Security Measures Using AI

Benefits of using AI

There are four benefits of using AI for Cybersecurity:

Reducing the cost of detection and response to breaches

Using AI for cybersecurity enables organisations to understand and reuse threat patterns to identify new threats. This leads to an overall reduction in time and effort to identify threats and incidents, investigate them, and remediate incidents.

Becoming faster at responding to breaches

A fast response is essential to protect an organisation from cyber attacks. According to the 2019 Capgemini's Reinventing Cybersecurity with Artificial Intelligence Report, using AI for cybersecurity, the overall time taken to detect threats and breaches is reduced by up to 12% and the time taken to remediate a breach or implement patches in response to an attack is also reduced by 12%. A small subset of organisations even managed to reduce these time metrics by more than 15%.

Increasing efficiency

Cyber analysts spend considerable time going through data logs and/or incident timesheets. Notwithstanding the significant workforce involved in cybersecurity, cyber analysts with deep knowledge of this field are rare. By using good data to analyse potential threats, AI enables cyber analysts to focus on works which only humans can do, such as analysing the incidents identified by the AI cybersecurity algorithms.

Making new revenue streams

As mentioned above, with the proliferation of IoT devices, the number, scope and scale of attacks has significantly increased. This creates opportunities for vendors offering cybersecurity services to manufacturers of IoT devices. Many players are taking advantage of the huge market opportunities.

Present Status of security measures using AI

As mentioned above, there are a lot of benefits to use AI for cybersecurity purposes, but at present AI can only be used to assist human work conducted for the purpose of cybersecurity, and human involvement is necessary. In other words, it is still necessary for human beings to continue to be responsible for customising teacher data to be learned by AI, determining issues to be solved by AI, and interpreting AI decisions.

In addition, decisions by AI use the "black box" model that lacks transparency as providing only input-output without the underlying rationale, and it is difficult to determine why the decision has been made. White-box models are the type of models which one can clearly explain how they behave and produce predictions and what the influencing variables are. However, they are yet to be put into practical use.

Security Measures Using AI and Fiduciary Duty of Care

Fiduciary duty of care

In many jurisdictions, directors and officers (hereinafter officers) of a company owe a fiduciary duty of care to the company. If an officer breaches a fiduciary duty of care in performing his/her role, the officer is liable to the company for the damage caused as a result.

Can it be considered that officers appropriately fulfil their fiduciary duty of care by introducing AI for cybersecurity purposes?

Use of AI for security measures and performance of fiduciary duty of care

As mentioned above, there are still some technical hurdles before AI can be used for security measures at present so that the introduction of AI itself in corporate procedures and strategies does not necessarily mean that the officer in charge of cybersecurity is appropriately discharging his/her duty and can be exculpated. Fairly common standards for determining the existence of a breach of fiduciary duty apply in many jurisdictions: whether the fiduciary duty of care is appropriately fulfilled is determined based on what would be normally expected from an ordinary officer having reasonable skills, experience and knowledge in a company of the same size and industry. Therefore, the introduction of AI does not necessarily mean that officers appropriately fulfilled their fiduciary duty of care under the present state of the art where it is clear that adequate and sufficient cybersecurity protection cannot be achieved through the mere introduction of the AI without appropriate human intervention and monitoring. Unless comprehensive security measures such as appropriate human intervention and human decision-making are introduced, cybersecurity measures could be determined to be insufficient. Accordingly, it is important for officers to build comprehensive cybersecurity system framework, and AI could be used to achieve this purpose as a part of structuring the cybersecurity system.

However, once these AI issues are resolved and the mere introduction of an AI-based cybersecurity system is widely recognised as appropriate for the cybersecurity protection of the company, it may be possible that an officer will be deemed to perform his fiduciary duty of care by simply introducing the appropriate AI-based cybersecurity system. If the absence of an AI-based cybersecurity system becomes a negative factor in the determination of a breach of fiduciary duty of care, it will be an incentive for all officers to introduce AI.

Future Prospects

As mentioned above, AI still has a lot of issues to overcome to form a stand-alone cybersecurity system. However, even at this early stage, in light of the benefits which could be derived from its use, AI will become an unavoidable tool in any efficient cyber defence strategy (especially where AI is being used in the attack).

The 2020 Tokyo Olympics and the 2025 World Exposition to be held in Japan are obvious targets. Major events have become attractive targets for "hacktivists" and fraudsters. The Rio de Janeiro Olympics in 2016 and the Pyeongchang Olympics in 2018 have been under heavy attacks (with allegations of cyberwarfare).

Cybersecurity is a hot topic and will be so for the years to come. Every state, business and individual will need to remain wary and watchful: no doubt AI will help.

Endnote

1. National center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity 2019*, May 23rd, 2019.

Akira Matsuda is an attorney-at-law (admitted in Japan and New York) and a partner at Iwata Godo heading the AI/TMT and Data Protection practice group. He is based in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions, as well as international disputes (litigation/arbitration), and advice on digital/TMT related matters. Mr. Matsuda regularly advises Japanese and foreign clients on data security issues (Japanese laws, Singapore PDPA, and EU GDPR) including on the structuring of global compliance systems. He also advises complicated cross-border corporate investigation matters.
He is a graduate of the University of Tokyo (LL.B.) and Columbia Law School (LL.M.).

Iwata Godo
Marunouchi Building 10F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6310
Japan

Tel: +81 3 3214 6205
Email: amatsuda@iwatagodo.com
URL: www.iwatagodo.com

Hiroki Fujita is an attorney-at-law (admitted in Japan) and associate at Iwata Godo. He is a member of the firm's AI/TMT and Data Protection practice group. His practice focuses on intellectual property law and IT. Mr. Fujita regularly advises clients across a broad range of industries, including electric power utilities and telecom carriers on data protection and cybersecurity issues. Mr. Fujita also advises clients on corporate matters, including mergers and acquisitions and corporate disputes (litigation/arbitration).
He is a graduate of Osaka University (LL.B.) and the Kyoto University School of Law (JD).

Iwata Godo
Marunouchi Building 10F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6310
Japan

Tel: +81 3 3214 6205
Email: hiroki.fujita@iwatagodo.com
URL: www.iwatagodo.com

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with about 70 attorneys and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection. Over the past few years, Iwata Godo has hosted a number of international seminars and conferences on data protection, often in coordination with "best friend" firms that are renowned firms and market leaders in their jurisdictions.

www.iwatagodo.com

IWATA GODO
Established 1902

Albania


Genc Boga


Armando Bode

Boga & Associates

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking constitutes a criminal offence in the Albanian jurisdiction. Article 192/b/1 of the "Criminal Code of the Republic of Albania" provides that unauthorised access or excess of authorisation to a computer system, or part of it, through violation of security measures is punishable by a fine or imprisonment for up to three years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2018, 11 cases have been recorded by the Prosecution body, two of which have ended with the sentencing of the accused, but no further details have been given.

Denial-of-service attacks
Article 293/c/1 of the "Criminal Code of the Republic of Albania" provides that the creation of serious and unauthorised obstacles to harm the function of a computer system, through insertion, damage, deformation, change or deletion of data is punishable with imprisonment of between three to seven years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2018, two cases have been recorded by the Prosecution body, but no details have been given on the cases.

Phishing
Article 143/b of the "Criminal Code of the Republic of Albania" states that adding, modifying or deleting computer data, or interfering in the functioning of a computer system, with the intention of ensuring for oneself or for third parties, through fraud, unfair economic benefits or causing a third party reduction of wealth is punishable by imprisonment for six months to six years and a fine from 60,000 Leke to 600,000 Leke. According to the Final Report of the General Prosecutor on the state of criminality for the year 2018, 52 cases have been recorded by the Prosecution body, but no details have been given on the cases.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Article 293/b of the "Criminal Code of the Republic of Albania" provides that damage, deformation, change or unauthorised deletion of computer data is punishable by imprisonment of between six months to three years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2018, 31 cases have been recorded by the Prosecution body, but no details have been given on the cases.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Article 293/ç of the "Criminal Code of the Republic of Albania" provides that manufacturing, keeping, selling, giving for use, distributing or any other action to place at disposal any equipment, including a computer program, computer password, access code or any other similar data created or adapted for breaching a computer system, or a part of it, with the aim of committing a criminal act, as provided in articles 192/b, 293/a and 293/c of the "Criminal Code of the Republic of Albania", is punishable by imprisonment for six months to five years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2018, there are no cases recorded by the Prosecution body.

Identity theft or identity fraud (e.g. in connection with access devices)
Even though the "Criminal Code of the Republic of Albania" does not explicitly mention or provide an article dedicated to identify theft, article 186/a states that modifying, deleting or omitting computer data, without the right to do so, in order to create false data with the intention of presenting and using them as authentic, even though the created data is directly readable or understandable, are all punishable by imprisonment of between six months to six years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2018, 19 cases have been recorded by the Prosecution body, eight of which has ended with the sentencing of the accused, but no details have been given.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Article 186/a/2 of the "Criminal Code of the Republic of Albania" provides that when the aforementioned criminal act, as described in the provision of identity theft above, is done by the person responsible for safekeeping and administering the computer data in cooperation more than once, or has brought forth grave consequences for the public interest, is punishable by imprisonment for three to 10 years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Article 293/b/2 of the "Criminal Code of the Republic of Albania" provides that damage, deformation, change or unauthorised deletion of computer data, when done with regard to military computer data, national security, public order, civil protection and healthcare, or in any other computer data with public importance, is punishable by imprisonment of between three to 10 years.

Failure by an organisation to implement cybersecurity measures
In virtue of Law No. 2/2017 "On cybersecurity", failure by an organisation to implement cybersecurity measures does not constitute a criminal offence. Article 21 of the Law "On cybersecurity" provides that failure to implement cybersecurity measures is considered an administrative violation and is punishable by a fine.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Convention "On cybercrime", ratified in Albania on 25.04.2002 through Law No. 8888, provides, in article 22, that Member States of the Convention must determine the jurisdiction in the cases where a cybercrime is committed in their territory or by a citizen of that state. Article 6/2 of the "Criminal Code of the Republic of Albania" provides that Albanian law is also applicable to Albanian citizens who commit a crime in the territory of another state, when the crime is at the same time punishable and as long as there is not any final decision by any foreign court for that crime. Also, article 7/a of the "Criminal Code of the Republic of Albania" states that the criminal law of the Republic of Albania is also applicable to foreign citizens who have committed a criminal act outside the territory of the Republic of Albania for which special laws or international agreements, of which the Republic of Albania is part of, determine the application of the Albanian criminal legislation.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Article 48 of the "Criminal Code of the Republic of Albania" provides mitigating circumstances for any penalty. These circumstances include, but are not limited to: a) when the criminal act is committed under the influence of psychic shock caused by provocation or unfair actions of the victim or any other person; b) when the criminal act is committed under the influence or unfair instruction of a superior; c) when the person responsible for the criminal act shows deep repentance; d) when the person has replaced the damage caused by the criminal act or has actively helped to erase or minimise the consequences of the criminal act; e) when the person presents him/herself before the competent bodies after committing the criminal act; and f) when the relations between the person who has committed the criminal act and the person who has suffered the consequences of the criminal act have returned to normal.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Article 74/a of the "Criminal Code of the Republic of Albania" states that distributing or offering to the public through computer systems materials that deny, minimise or significantly approve or justify acts which constitute genocide or crimes against humanity is punishable by imprisonment of between three to six years. Also, article 84/a of the "Criminal Code of the Republic of Albania" provides that serious threats to kill or seriously injure a person through computer systems because of ethnicity, nationality, race or religion are punishable with a fine or imprisonment for up to three years. Article 119/a of the "Criminal Code of the Republic of Albania" states that offering or distributing to the public through computer systems materials with racist or xenophobic content constitutes an administrative violation and is punishable by a fine or imprisonment for up to two years. Article 119/b of the "Criminal Code of the Republic of Albania" provides that a public insult involving ethnicity, nationality, race or religion through a computer system constitutes an administrative violation and is punishable by a fine or imprisonment for up to two years.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

1. The Convention "On cybercrime", ratified in Albania on 25.04.2002 by Law No. 8888.
2. Law No. 7895, dated 27.01.1995, "Criminal Code of the Republic of Albania", as amended.
3. Law No. 2/2017 "On cybersecurity".
4. Law No. 9918, dated 19.05.2008, "On electronic communications in the Republic of Albania", as amended.
5. Law No. 9887, dated 10.03.2008, "On protection of personal data", as amended.
6. Law No. 8457, dated 11.02.1999, "On classified information 'Secrets of State'", as amended.
7. Law No. 9880, dated 25.02.2008, "On electronic signatures", as amended.
8. The Decision of Council of Ministers No. 141, dated 22.02.2017, "On organising a functioning of the national authority for electronic certification and cybersecurity".

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Article 8 of the Law "On cybersecurity" specifies that operators of critical infrastructure of information are obliged to implement the requirements of safety measures and to also document their implementation. Article 9/3 of the Law "On cybersecurity" provides that the Responsible Authority for Electronic Certification and Cybersecurity (herein the "Authority") determines, through a regulation, the content and method of documenting the safety measures. To the best of our knowledge, no such regulation exists.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Article 9 of the Law "On cybersecurity" provides a list of safety measures and divides them into two groups: organisational measures; and technical measures. As specified above, the Authority determines, through a regulation, the content and method of documenting the safety measures. To date, no such regulation exists.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

To the best of our knowledge, no such regulation exists.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Article 11 of the Law "On cybersecurity" determines that operators of critical infrastructure of information and operators of important infrastructure of information are required to report immediately after they detect cybersecurity Incidents to the National Authority on Electronic Signature and Cybersecurity. The Authority determines by regulation the types and categories of cybersecurity Incidents, as well as the format and elements of the cybersecurity Incident report. In the case of cybersecurity Incidents and attacks on constitutional, security and defence institutions, the Authority reports immediately to the leaders of these institutions on the issues and measures to be taken.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

As we mentioned above, it is required by the law to immediately report after organisations detect cybersecurity Incidents.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

To the best of our knowledge and after reviewing the legislation, there are no provisions with regard to this situation.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses to questions 2.5 to 2.7 do not change regardless of the information included.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Article 8 of the Law "On cybersecurity" provides that operators of critical infrastructure of information and operators of important infrastructure of information are obliged to implement the safety measures and also document their implementation. Furthermore, the aforementioned operators are obliged to implement the requirements of the safety measures during the establishment of the infrastructure.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Article 22 of the Law "On cybersecurity" states that in case of non-compliance with the requirements specified in the law, the Authority issues fines from 20,000 Leke to 800,000 Leke.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

To the best of our knowledge, there are no examples of enforcement action taken in cases of non-compliance with the abovementioned requirements.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
To the best of our knowledge, there are no provisions in this regard.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
To the best of our knowledge, there are no provisions in this regard.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
To the best of our knowledge, there are no provisions in this regard.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

There is no difference as regards the variety of measures taken across different business sectors, because the Law "On cybersecurity" is applied the same regardless of the business sector.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Law "On cybersecurity" is the only one governing cybersecurity for all organisations, private or public, in the Republic of Albania.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The Law "On cybersecurity" does not elaborate on this point but, nevertheless, this is a matter of regulation inside the company.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

To the best of our knowledge, there is no obligation to fulfil these requirements. The Authority shall draft, approve and publish the necessary regulations to complete the legislative frame for cybersecurity within 12 months of the date of the law's approval.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The Law "On cybersecurity", even though it does not clearly mention companies, provides the obligation to report to the competent authorities. However, the "Code of Criminal Procedure of the Republic of Albania" demands disclosure when legally asked by the Prosecution, be it through an order or a court decision.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

To the best of our knowledge, companies are not subject to any other specific requirements under Applicable Laws in relation to cybersecurity.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

For a civil action to be brought in relation to any Incident, it is necessary to provide the element of damage caused by a person committing an illegal action and provide evidence as to the causality of this action. It is also necessary to identify the source or the person responsible for the Incident.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

To the best of our knowledge, there are no specific examples of cases brought in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The Law "On cybersecurity" does not provide any specifics in this regard, but there is potential liability in tort in relation to an Incident in virtue of the "Civil Code of the Republic of Albania", as specified above.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

To the best of our knowledge, organisations are not prohibited from taking out insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations to insurance coverage against specific types of loss, such as business interruption.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Article 9 of the Law "On cybersecurity" states that responsible bodies should take the necessary measures to manage and monitor the safety of human resources and people's access.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

To the best of our knowledge and after carefully reviewing the current Albanian legislation on the matter, there are no prohibitions in this regard.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Structures for cybercrime at the County Directory Police and General County Directory Police are responsible for investigating any crimes related to cybersecurity. In addition, the State Police has made available to the public a website (http://www.policia.al/denonco/) where every person can report in real-time any criminal act related to cybercrimes. The Authority is also responsible for investigating any reported crimes related to cybersecurity.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

To the best of our knowledge, there are no requirements under the Applicable Laws for organisations to implement backdoors in their IT systems.

Genc Boga is the founder and Managing Partner of Boga & Associates operating in Albania and Kosovo.
Mr. Boga has solid expertise as an advisor to banks, financial institutions and international investors operating in the energy, infrastructure, technology and real estate sectors.
Thanks to his experience, Mr. Boga acts as a legal advisor on a regular basis for the most important international financial institutions and foreign investors intending to invest in Albania and Kosovo.
He is regularly engaged by EBRD, IFC and the World Bank in various investment projects in Albania and Kosovo.
Mr. Boga is continuously ranked as a leading lawyer in Albania by the most reputable international directories such as *Chambers and Partners*, *The Legal 500* and *IFLR 1000*.
He is fluent in English, French and Italian.

Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 225 1050
Email: gboga@bogalaw.com
URL: www.bogalaw.com

Armando Bode is an Associate at Boga & Associates, which he joined in 2015.
He assists foreign investors (including Fortune 500 companies) on various business law aspects, including corporate, compliance and regulatory implications. Armando is also a licensed Trademark Attorney and regularly advises clients operating in technology, fashion and food industries in IP, IT and data protection law assignments.
In addition to his client-related work, Armando is continuously publishing for various law journals and magazines within his areas of expertise and also assists different business associations with *pro bono* advice.
Armando holds a Bachelor of Laws (2014) and a Master of Science in Public Law (2016) from the University of Tirana.
In addition to Albanian, he speaks fluent English and Italian.

Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 225 1050
Email: abode@bogalaw.com
URL: www.bogalaw.com

Boga & Associates, established in 1994, has emerged as one of the premier law firms in Albania and Kosovo, earning a reputation for providing the highest quality of legal, tax and accounting services to its clients. Until May 2007, the firm was a member firm of KPMG International and the Senior Partner/Managing Partner, Mr. Genc Boga, was also the Senior Partner/Managing Partner of KPMG Albania.
The firm's particularity is linked to the multidisciplinary services it provides to its clients through an uncompromising commitment to excellence. Apart from the widely consolidated legal practice, the firm also offers the highest standards of expertise in tax and accounting services, with keen sensitivity to the rapid changes in the Albanian and Kosovo business environment.
The firm delivers services to leading clients in major industries, banks and financial institutions, as well as to companies engaged in insurance, construction, energy and utilities, entertainment and media, mining, oil and gas, professional services, real estate, technology, telecommunications, tourism, transport, infrastructure and consumer goods.
The firm is continuously ranked as a "top tier firm" by major directories: *Chambers Global*, *Chambers Europe*, *The Legal 500*, and *IFLR 1000*.

www.bogalaw.com

BOGA & ASSOCIATES
LEGAL • TAX • ACCOUNTING

Australia


Dennis Miralis


Phillip Gibson


Jasmina Ceic

Nyman Gibson Miralis

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

In Australia, unauthorised access to computer systems is criminalised by both State and Federal legislation. In the Federal jurisdiction, hacking is criminalised under the Criminal Code Act 1995 (Cth) ("the Code"). Most commonly, persons suspected of engaging in cybercrime are charged pursuant to the Code, given its universal application in all States and Territories in Australia.

The recent report published by the Five Eyes intelligence alliance details the public availability of hacking tools and the worldwide proliferation of hacking practices. Hacking activity is carried out by both sophisticated organised crime syndicates as well as independent amateur perpetrators. The tools detailed fall into five categories: Remote Access Tools; Web Shells; Credential Stealers; Lateral Movement Frameworks; and Command and Control Obfuscators.

Persons suspected of unauthorised access to computer systems are charged pursuant to s. 478.1 of the Code, which provides for the offence of "Unauthorised access to, or modification of, restricted data". The offence is comprised of three elements of proof. The offence is committed if: a person causes any unauthorised access to, or modification of, restricted data; the person intends to cause the access or modification; and the person knows that the access or modification is unauthorised. The maximum penalty for a contravention of s. 478.1 of the Code is two years' imprisonment.

Denial-of-Service attacks

Denial-of-Service attacks ("DoS attacks") or Distributed Denial of Service attacks ("DDoS attacks") are criminalised by s. 477.3 of the Code, which provides for the offence of "Unauthorised impairment of electronic communication". The offence is comprised of two elements. The offence is committed if a person causes any unauthorised impairment of electronic communication to or from a computer and the person knows that the impairment is unauthorised. The maximum penalty for a contravention of s. 477.3 of the Code is 10 years' imprisonment.

Phishing

Phishing, being a form of online fraud, is criminalised under the Code in instances where the victim is said to be a Commonwealth entity. When the victim is a member of the public, charges are brought under parallel State or Territory legislation.

Commonwealth fraud prosecution encompasses a wide variety of offending conduct, including phishing-style offences which would affect a Federal government body. Depending on the subsequent financial gain or loss suffered subsequent to the activity, the below charges are available:

- S. 134.2(1) – obtaining a financial advantage by deception.
- S. 135.1(1) – general dishonesty – obtaining a gain.
- S. 135.1(3) – general dishonesty – causing a loss.
- S. 135.1(5) – general dishonesty – causing a loss to another.

For the charge to be proven, the prosecution must establish that the accused obtains or causes a financial advantage, gain or loss by way of deception or dishonesty. The maximum penalty for each offence is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware is criminalised by s. 478.2 of the Code, which provides for the offence of "Unauthorised impairment of data held on a computer disk etc.". The offence is comprised of three elements. The offence is committed if: a person causes any unauthorised impairment of the reliability, security or operation of data held on a computer disk, a credit card or another device used to store data by electronic means; the person intends to cause the impairment; and the person knows that the impairment is unauthorised. The maximum penalty is two years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Possession or use of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.3 of the Code, which provides for the offence of possession or control of data with intent to commit a computer offence. The offence is comprised of two elements. The offence is committed if: a person has possession or control of data; and the person has that possession or control with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of the Code or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.3 of the Code is three years' imprisonment.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity crime, and in particular identity fraud offences, are criminalised by Division 372 of the Code. Particular acts that are criminalised include dealing in identification information, dealing in identification information that involves use of a carriage service, possession of identification information and possession of equipment used to make identification information. The offence of "Dealing in identification information that involves use of a carriage service" is most relevant to cybercrime. It is criminalised by s. 372.1A of the Code and is comprised of four elements. The offence is committed if: a person deals in identification information; the person does so using a carriage service; the person intends that any person will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of committing an offence or facilitating the commission of an offence; and the offence is an indictable offence against the law of the Commonwealth, an indictable offence against a law of a State or Territory or a foreign indictable offence. The maximum penalty is five years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is criminalised by s. 478.1 of the Code. As the offence is committed if a person modifies restricted data, modification is defined in the Code as the alteration or removal of the data held in a computer, or an addition of the data held in a computer, the unauthorised copying of data from a computer would contravene the offence provision.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Part 10.6 of the Code creates offences related to telecommunication services. They include offences relating to dishonesty with respect to carriage services and interference with telecommunications.

Failure by an organisation to implement cybersecurity measures
See the discussion below in relation to corporate governance.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Extended geographical jurisdiction applies to offences under Part 10.7 of the Code (Divisions 477 and 478).

A person will not commit offences under that Part unless: the conduct constituting the alleged offence occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offences occurs wholly outside Australia and a result of the conduct occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offence occurs wholly outside Australia and at the time of the alleged offence, the person is an Australian citizen or at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or all of the following conditions are satisfied: the alleged offence is an ancillary offence; the conduct constituting the alleged offence occurs wholly outside Australia; and the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia or wholly or partly on-board an Australian aircraft or an Australian ship.

Australia is also a signatory to the *Council of Europe Convention on Cybercrime* (the Budapest Convention), a multilateral instrument intended to facilitate intergovernmental cooperation in the regulation, investigation and enforcement of cybercrime. Chapter III of the treaty makes provision for cooperation among Parties "to the widest extent possible". Cooperation is not limited with respect to cybercrime (offences against and by means of computers) but also includes any example of crime involving electronic evidence. Increasingly, Australian government agencies are operating as part of cross-border investigations, often working collaboratively with their international counterparts in parallel investigations.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The *Crimes Act 1914* (Cth) prescribes the sentences applicable to breaches of Federal legislation, such as the Code. Relevant matters for consideration on sentence are set out as a non-exhaustive list of factors under s. 16A of the Crimes Act 1900 (Cth). Matters that generally will mitigate a penalty include the timing of any guilty plea, the offender's character, the offender's prior record, assistance provided by the offender to the authorities and the offender's prospect of rehabilitation and likelihood of reoffending. Notification would be a matter that could be taken into account by a sentencing court as a factor of mitigation.

A number of the offences particularised above cannot be "attempted"; they must actually be committed. For example, a person cannot attempt to commit the offence of "Unauthorised access, modification or impairment with intent to commit a serious offence".

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

A number of criminal offences may arise in relation to cybersecurity or the occurrence of an Incident, although they are best understood as tangential or ancillary to cybersecurity or the occurrence of an Incident. For example, there have been prosecutions for offences such as blackmail where an offender has used material obtained as a result of a breach of confidence to blackmail the owner by threatening to release that material online.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The following laws in New South Wales relate to cybersecurity: the *Privacy Act* (Cth) ("Privacy Act"); the *Crimes Act 1914* (Cth); the *Security of Critical Infrastructure Act 2018* (Cth); the *Criminal Code 1995* (Cth); and the *Telecommunications (Interception and Access) Act 1979* (Cth).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The *Security of Critical Infrastructure Act 2018* (Cth), which commenced on 11 July 2018, seeks to manage national security risks of sabotage, espionage and coercion posed by foreign entities. The Act was implemented as a response to technological changes that have increased cyber connectivity to critical infrastructure. The Australian Government considers "the responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community" as being shared "between owners and operators of critical infrastructure, state and territory governments and the Australian Government". The Act applies to approximately 165 specific assets in the electricity, gas, water and ports sectors.

The Act establishes a Register of Critical Infrastructure Assets, empowers the Secretary of the Department of Home Affairs with an information-gathering power (whereby certain information can be requested of direct interest holders, responsible entities and operators of critical infrastructure assets) and a Minister has the power to issue a direction to an owner or operator of critical infrastructure assets to mitigate national security risks.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

See generally the answer to question 4.3 below in respect of the NDB Scheme.

The Australian Securities and Investments Commission ("ASIC") provides guidance to Australia's integrated corporate markets, financial services and consumer regulator, and provides guidance to organisations through its "cyber reliance good practices". The good practices recommend, *inter alia*, periodic review of cyber strategy by a board of directors, using cyber resilience as a management tool, for corporate governance to be responsive (i.e. keeping cybersecurity policies and procedures up to date), collaboration and information sharing, third-party risk management and implementing continuous monitoring systems.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

See the answer to question 4.3 below.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

See the answer to question 4.3 below.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Subject to the restrictions in the Applicable Laws (such as the Privacy Act), organisations are permitted to voluntarily share information related to an Incident or potential Incidents with a regulatory or other authority and other private sector or trade associations.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See the answer to question 4.3 below.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

See the answer to question 4.3 below.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Office of the Australian Information Commissioner ("OAIC") is an independent statutory agency within the Attorney-General's Department. The OAIC has three functions; namely, privacy functions conferred by the Privacy Act, freedom of information functions, such as reviewing the decisions made by agencies and ministers pursuant to the *Freedom of Information Act 1982* (Cth), and government information policy functions conferred by the *Australian Information Commissioner Act 2010* (Cth).

In relation to its privacy functions, the OAIC has the power to commence investigations, conduct privacy performance assessments, request an entity to develop an enforceable code, direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function and recognise external dispute resolution schemes to handle privacy-related complaints.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

See the answer to question 4.3 below.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The OAIC reported that, in response to Commissioner-initiated investigations, enforceable undertakings were accepted by three Australian Privacy Principles ("APP") entities over the 2017–2018 period, namely the Australian Red Cross Blood Service, Precedent Communications Pty Ltd and the Department of Health.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are presently no laws in Australia which prohibit the use of a Beacon or near-field communication technology.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are presently no laws in Australia which prohibit the use of Honeypot technology or similar autonomous deception measures.

Honeypots are a cybersecurity tool used by both public and private agencies to detect network attacks.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are presently no laws in Australia which prohibit the use of Sinkhole technology. The malicious use of Sinkhole methods to steer legitimate traffic away from its intended recipient may, however, constitute an offence under s. 477.3 of the Code.

Sinkholes can be lawfully used as a defensive practice for research and in reaction to cyber-attacks. In this capacity, Sinkholes are a tool used by both public and private agencies.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors in New South Wales. The Notifiable Data Breaches ("NDB") Scheme, for example, only requires not-for-profit businesses with an annual turnover of more than AUD $3 million to report data breaches.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Part IIIA of the Privacy Act specifically regulates the handling of personal information about individuals' activities in relation to consumer credit, including the types of personal information that credit providers can disclose. All credit reporting bodies (defined in ss 6 and 6P as a business that involves collecting, holding, using or disclosing personal information about individuals for the purposes of providing an entity with information about the creditworthiness of an individual) are subject to Part III.

Part 13 of the Telecommunications Act 1997 (Cth) regulates carriers and carriage service providers in their use and disclosure of personal information. Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (Cth) requires providers of telecommunications services in Australia to collect and retain specific types of data for a minimum period of two years and must comply with the Privacy Act in relation to that data.

See generally the answer to question 4.3 below for more information. The NDB Scheme in Part IIIC of the Privacy Act requires the telecommunications and financial services sectors to take steps to secure personal information. These sectors must notify individuals whose personal information is involved in a data breach that is likely to result in serious harm, and must also notify the OAIC.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

A failure by a company to prevent, mitigate, manage or respond to an Incident may result in breaches of provisions of the *Corporations Act 2001* (Cth). The *Corporations Act 2001* (Cth) imposes duties on directors to exercise powers and duties with the care and diligence that a reasonable person would. A director who ignores the real possibility of an Incident may be liable for failing to exercise their duties with care and diligence.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Presently, the Applicable Laws do not require companies to designate a CISO, establish a written Incident response plan or policy, conduct periodic cyber risk assessments or perform penetration tests or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

In February 2018, the Privacy Amendment (Notifiable Data Breaches) Act 2017 amended the Privacy Act to require APP entities to, as soon as practicable, provide notice to the OAIC and affected individuals of an "eligible data breach", where there are reasonable grounds to believe that an "eligible data breach" has occurred. This process is called the Notifiable Data Breaches Scheme.

Eligible data breaches arise when: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; this unauthorised disclosure of personal information, or loss of personal information is likely to result in serious harm to one or more individuals; and the entity has not been able to prevent the likely risk of serious harm with remedial action. Indicators such as malware signatures, observable network vulnerabilities and other 'red-flag' technical characteristics may represent reasonable grounds for an APP entity to form a belief that an eligible data breach has occurred.

The OAIC expects APP entities to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm.

The notification to the OAIC and to the affected individual must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps individuals should take in response to the data breach.

A failure to comply with the notification obligations can result in the imposition of substantial civil penalties. A serious or repeated interference with privacy attracts a fine of 2,000 penalty units, currently AUD $420,000.00. The maximum penalty that a court can order for a body corporate is five times the amount listed in the civil penalty provision, currently a maximum of AUD $2.1 million.

The Privacy Act also confers a number of additional enforcement powers on the OAIC, including accepting an enforceable undertaking, bringing proceedings to enforce an enforceable undertaking, making a determination, making orders that the APP entity must redress any loss or damage suffered by the complainant and that the complainant is entitled to payment of compensation for such loss or damage, bringing proceedings to enforce a determination, delivering a report to the responsible Minister and seeking an injunction.

Under the Privacy Act, an APP entity is defined as an "agency" or "organisation". "Agency" includes a Minister, a Department, and most government bodies; and "organisation" means an individual, a body corporate, a partnership, any other unincorporated association or a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

In the performance of its role as an Australian intelligence and security agency, and through its use of foreign signals intelligence and offensive cyber operations, the Australian Signals Directorate ("ASD") may also detect security weaknesses or vulnerabilities in technology that are unknown to the vendor and that may pose a threat to Australians and Australian systems. The ASD will disclose these vulnerabilities only in circumstances where disclosure is determined to be in the Australian national interest.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Australian Privacy Principles contained in schedule 1 of the Privacy Act provide for the manner in which APP entities must handle and use personal information. There are 13 privacy principles, covering: open and transparent management of personal information; anonymity and pseudonymity; collection of solicited personal information; dealing with unsolicited personal information; notification of the collection of personal information; the use or disclosure of personal information; direct marketing; cross-border disclosure of personal information; adoption, use or disclosure of government-related identifiers; quality of personal information; security of personal information; access to personal information; and the correction of personal information. The APPs are not prescriptive, and an APP entity must consider how the principles apply to its own situation.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Australian common law does not recognise a general right of privacy. The equitable cause of action for breach of confidence may provide a remedy for invasions of privacy. Traditionally, the elements are that information must be confidential, information must have been imparted in circumstances importing an obligation of confidence and there must be an unauthorised use of that information. The current doctrine of breach of confidence does not currently entertain cases of wrongful intrusion, as opposed to cases of wrongful disclosure of confidential information.

The Privacy Act regulates the way Commonwealth agencies handle personal information. A person may obtain an injunction in the Federal Circuit Court against a Commonwealth agency that engages in, or proposes to engage in, conduct that is in breach of the Privacy Act. An action cannot be brought against an individual acting in their own capacity. A person may apply to the Court for an order that an entity pay compensation for loss or damage suffered by the person if a civil penalty has been made against the entity, or the entity is found guilty of an offence under the Privacy Act.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

No relevant civil proceedings have been brought by individuals in relation to an Incident. Given the evolution of the doctrine of breach of confidence, it is likely such cases will be forthcoming.

Investigations conducted by the OAIC most commonly result in out-of-court outcomes. For example, a joint investigation conducted by the Australian Privacy Commissioner and the Privacy Commissioner of Canada into a highly publicised hacking breach of confidential data held by online adult dating service Ashley Madison, resulted in an enforceable undertaking being entered into by the company pursuant to s. 33E of the Privacy Act.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The High Court in *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 sanctioned the recognition of a tort of invasion of privacy. Judge Hampel in the case of *Doe v ABC* (2007) VCC 281 imposed liability in tort for the invasion of the plaintiff's privacy. Such reasoning may apply to an action in relation to an Incident.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations are permitted to take out insurance against Incidents in Australia. This includes breaches of the Privacy Act.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limits specifically targeted at losses associated with Incidents. Numerous entities offer insurance for data breach, business interruption, email forgery, ransomware attacks, costs of rebuilding an IT system, theft of crypto-currencies and legal fees associated with the investigation of Incidents. Coverage is governed generally by the *Insurance Act 1973* (Cth), the *Insurance Contracts Act 1984* (Cth), the *Corporations Act 2001* (Cth) and the common law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

At the Commonwealth level, the *Surveillance Devices Act 2004* (Cth) makes provision for the use of surveillance devices by Federal law enforcement officers.

The *Workplace Surveillance Act 2005* (NSW) (and uniform legislation in all other Australian States and Territories) restricts the use of both overt and covert forms of surveillance of an employee by employers and other members of the public. Surveillance can include computer surveillance. Significant penalties are imposed for breaches of the Act, including imprisonment.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

On 13 December 2017, the Treasury Laws Amendment (Whistleblowers) Bill 2017 (Cth) was introduced in Parliament. The Bill repeals the former whistleblower regime and creates a revised and consolidated whistleblower protection regime in the Corporations Act 2001 (Cth) and a whistleblower protection regime in the Taxation Administration Act 1953 (Cth).

The level of protection afforded to whistleblowers by the new law has been strengthened in a number of key areas including:

- strengthening the requirement of confidentiality of a whistleblower's identity;
- ensuring that persons, including regulators, cannot be required to disclose the identity of a whistleblower to a court or tribunal without a court order;
- strengthening the immunities provided to whistleblowers and ensuring that they are not subject to any civil, criminal or administrative liability following the provision of a qualifying disclosure; and
- broadening the prohibition against victimisation of whistleblowers and increasing the relevant penalties for instances of victimisation.

A qualifying disclosure can be made for information concerning misconduct, including criminal conduct or breach of legal obligation in relation to a regulated entity or related corporate entity.

The regime does not limit but, conversely, facilitates the reporting of cyber risks, security flaws, Incidents or potential Incidents to which there is an element of corporate culpability.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

A number of well-established legal investigatory powers are deployed by law enforcement authorities when investigating an Incident. These powers can include the issuing of search warrants, the seizure of IT equipment for forensic analysis, decryption (whether at encrypted or decrypted data points) and the compulsory examination of suspects in certain circumstances.

The ASD assumes responsibilities for defending Australia from global threats and advances its national interests through the provision of foreign signals intelligence, cybersecurity and offensive cyber operations as directed by the Australian Government. One of the express strategic objections of the ASD is to provide advice and assistance to law enforcement. To this end, the ASD can collaborate with the Federal, State and Territory police forces in relation to matters of national interest, including emerging areas such as cyberterrorism.

See the answer to question 8.2 below for statutory notices which can be issued by law enforcement agencies to access data held by designated communications providers.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

On 8 December 2018, the Federal Parliament passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. The Act provides for the facilitation of covert access to data for the purposes of disrupting and investigating criminal activity, as well as establishing a framework to facilitate lawful assistance from communications providers.

The legislation allows various Australian law enforcement and intelligence agencies to make a Technical Assistance Notice ("TAN"), ordering designated communications providers to provide data or assistance in relation to criminal investigations or matters of security. This may include access to encryption keys or provision of decrypted data. Similarly, Technical Capability Notices ("TCN") can

be issued, mandating that a designated communications provider establish new capability to intercept and decrypt communications that would otherwise be encrypted or inaccessible.

The above notices may be issued in a broad variety of circumstances, including the enforcement of criminal laws and laws imposing pecuniary penalties, either in Australia or in a foreign country, or if it is in the interests of Australia's national security, Australia's foreign relations, or Australia's national economic well-being.

A designated communications provider, including an individual employed or acting on behalf of such providers, who has been compelled to provide data or assistance under a computer access warrant and fails to do so, may face up to 10 years' imprisonment, a fine of up to 600 penalty units (currently AUD $126,000) or both.

S. 3LA of the *Crimes Act 1914* (Cth) also provides law enforcement authorities a mechanism by which a person must provide information or assistance that is reasonable and necessary to allow a constable to: access data held in, or accessible from, a computer or data storage device that is on warrant premises or that has been moved to a place for examination under subsection 3K(2) of the *Crimes Act 1914* (Cth); copy data held in, or accessible from, a computer or storage device; and convert into documentary form, or another form intelligible to a constable, data held in, or accessible from, a computer or data storage device, or data held in a data storage device to which the data was copied, or data held in a data storage device removed from warrant premises under subsection 3L(1A) of the *Crimes Act 1914*.

Acknowledgment

The authors would like to thank Damien Mahon, Solicitor, for his invaluable contribution to the writing of this chapter. Damien assists the Partners on international criminal law cases and cross-border investigations.

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include cybercrime, global investigations, proceeds of crime, bribery and corruption, anti-money laundering, worldwide freezing orders, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/dennis-miralis-partner-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Phillip Gibson is one of Australia's leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law. Phillip has significant experience in transnational cases across multiple jurisdictions, often involving: white-collar and corporate crime; asset forfeiture; money laundering and proceeds of crime; extradition; mutual legal assistance; Royal Commissions; bribery and corruption; and ICAC and Crime Commission matters. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/phillip-gibson-partner-specialist-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: pg@ngm.com.au
URL: www.ngm.com.au

Jasmina Ceic is an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system, with a specialist focus on serious matters that proceed to Trial in the Superior Courts, as well as conviction and sentence Appeals heard in the Court of Criminal Appeal. She has represented and advised persons and companies being investigated for white-collar and corporate crime, complex international fraud and transnational money laundering.
Full biography: https://ngm.com.au/our-team/jasmina-ceic-senior-associate/.

Nyman Gibson Miralis
Suite 8, Level 2
154 Marsden Street
Parramatta NSW 2150
Australia

Tel: +61 2 9633 4966
Email: jc@ngm.com.au
URL: www.ngm.com.au

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.
Our international law practice focuses on cybercrime, white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, international asset freezing or forfeiture, extradition and mutual legal assistance law.
Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, British Virgin Islands, New Zealand and South Africa.

www.ngm.com.au

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

Belgium


Roeland Lembrechts


Bart Van den Brande

Sirius Legal

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking, as an unauthorised access to an IT system, is criminalised under article 550*bis* of the Belgian Criminal Code (BCC).

The first distinction that has to be made is between the basic crime (external and internal) and the subsequent actions.

External hacking happens when a person not possessing any access rights knowingly intrudes in or maintains access to an IT system. The penalties are between six months and two years of imprisonment and/or a fine between 208 EUR and 200,000 EUR. In cases where fraudulent purpose is found, the maximum imprisonment is increased to three years.

Internal hacking happens when a person, who has access rights, exceeds those rights with a fraudulent purpose or with the purpose to cause damage. The penalties are between six months and three years of imprisonment and/or a fine between 208 EUR and 200,000 EUR.

Subsequent actions are aggravating circumstances with increased penalties: imprisonment between one and five years and/or a fine between 208 EUR and 400,000 EUR. Subsequent actions can be stealing data, damaging an IT system or taking over an IT system to hack another system.

Instructing or commissioning a third party to commit hacking is punishable between six months and five years of imprisonment and/or a fine between 800 EUR and 1,600,000 EUR.

Knowingly disseminating or using data obtained as a result of hacking is punishable with imprisonment between six months and three years and/or a fine between 208 EUR and 800,000 EUR.

Denial-of-service attacks
Denial-of-service attacks are criminalised as computer sabotage, i.e. "knowingly and without authorization, directly or indirectly introducing, altering or deleting data in an IT system, or changing by any other technological means the normal use of any data in an IT system" (article 550*ter*, §1 BCC).

The penalties are between six months and three years of imprisonment and/or a fine between 208 EUR and 200,000 EUR. If real damage is caused to the IT system, the maximum imprisonment is increased to five years and the maximum fine and 600,000 EUR.

In cases with fraudulent purpose or intention of causing harm, the penalties are increased to a maximum of five years' imprisonment. The same increase applies to attacks against critical infrastructures.

Causing a disruption of the correct working of the IT system is an aggravating circumstance: penalties are increased to between one and five years' imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Phishing
This is, in most cases, punishable by article 504*quater* BCC, i.e. "with fraudulent purpose, acquiring an unlawful economic advantage for himself or for someone else, by introducing, modifying, deleting data that is stored, processed or transferred in an IT system, by means of an IT system or changing the normal use of data in an IT system by any other technological means".

The penalties are between six months and five years of imprisonment and/or a fine between 208 EUR and 800,000 EUR. An attempt is punishable by six months to three years of imprisonment and/or a fine between 208 EUR and 400,000 EUR.

Phishing may also be punishable under article 145, §3, 1° of the Electronic Communications Act of 13 June 2005, prohibiting the fraudulent initiation of electronic communications, by means of an electronic communications network, with the intent to obtain an illegitimate economic advantage (for oneself or for another). This criminal offence is punishable between one and four years of imprisonment and/or a fine between 4,000 EUR and 400,000 EUR.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This is an act of computer sabotage (article 550*ter*, §1 BCC).

The same criminal penalties apply as those applicable to denial-of-service attacks.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
It is a criminal offence on its own to illegitimately possess, produce, sell, procure for use, import, distribute, disseminate or otherwise make available any instrument, including computer data, designed or adapted to enable hacking (article 550*bis*, §5 BCC) or computer sabotage (article 550*ter*, §4 BCC).

The penalties are between six months and three years of imprisonment and/or a fine between 208 EUR and 800,000 EUR.

When this offence intercepts communication that is not publicly accessible, the penalties are between six months and two years of imprisonment and/or a fine between 1,600 EUR and 80,000 EUR (article 314*bis*, §2*bis* BCC). If committed by a public officer, the penalties are between six months and three years of imprisonment and/or a fine between 4,000 EUR and 160,000 EUR (article 259*bis*, §2*bis* BCC).

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft is often a precursor to another criminal offence, e.g. theft, fraud, computer fraud, hacking or computer sabotage committed by using the stolen identity.

Identity fraud may directly be a criminal offence only if the fraud relates to the appropriation of the capacity of a civil servant or military functions, nobility titles, the title of attorney-at-law or the public use of a false family name (articles 227–231 BCC). Penalties are usually limited to fines (up to 8,000 EUR).

Additionally, identity theft or fraud can be qualified as an illegitimate process of personal data. Depending on the specific qualification, these offences are punished by the Belgian GDPR Act of 30 July 2018 with a fine between 2,000 EUR and 120,000 EUR (article 222), 800 EUR to 160,000 EUR (article 227) or 4,000 EUR to 240,000 EUR (article 223).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

There is no general qualification for electronic theft. Although there has been discussion, case law ruled that, e.g., theft of computer data can be punished under the general definition of theft (article 431 BCC).

As a subsequent action to theft, according to articles XI.304 and XV.105 of the Belgian Economic Law Code, knowingly putting an unlawful copy of a computer program on the market or having it for commercial purposes, or putting on the market or having resources for commercial purposes that are exclusively intended for the unauthorised person to facilitate the removal or circumvention of technical provisions to protect a computer program is punishable with imprisonment between one and five years.

Other intellectual properties are secured by articles XV.103–XV.106 of the Belgian Economic Law Code with imprisonment between one and five years and/or a fine between 4,000 EUR and 800,000 EUR in cases of infringement (piracy and counterfeit) with fraudulent and malicious purpose.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article 210*bis* BCC punishes the committing of falsehood, i.e. "by entering data that are stored, processed or transferred through an IT system, into an IT system, to change, to delete or to change the possible use of data in an IT system with any other technological means, which changes the legal scope of such data".

The penalties are between six months and five years of imprisonment and/or a fine between 208 EUR and 800,000 EUR.

Failure by an organisation to implement cybersecurity measures

The Belgian Cyber Security Act of 7 April 2019, implementing the NIS-Directive 2016/1148, requires several obligations concerning security, notification and information from digital service providers and operators of essential services.

Failure to comply results in the following penalties:

- security: imprisonment between eight days and one year and/or a fine between 208 EUR and 240,000 EUR;
- notification: imprisonment between eight days and one year and/or a fine between 208 EUR and 160,000 EUR; and
- information: imprisonment between eight days and one year and/or a fine between 208 EUR and 400,000 EUR.

For hardware and software providers, product and service security is governed by the product liability rules under articles IX.1–IX.11 of the Belgian Economic Law Code. Failure to comply with product liability rules is punished with a fine between 208 EUR and 200,000 EUR. In cases involving cybersecurity, certification will be important under Regulation 2019/881 of 17 April.

Article 88 of the Belgian GDPR Act stipulates an obligation to implement appropriate technical and organisational measures necessary for the protection of personal data against accidental or unauthorised destruction, against accidental loss, etc. Failures are punished with a fine between 800 EUR and 80,000 EUR (article 226). Not taking adequate measures can also be punished by article 83, §4 GDPR with an administrative fine.

Article 26, §1 of the Act of 1 July 2011, concerning the security and protection of critical infrastructures (CIA), imposes a term of imprisonment between eight days and one year and/or a fine between 208 EUR and 80,000 EUR in case of a breach of any obligation under this Act, including the establishment and execution of a security plan (which may include cybersecurity measures).

Failure of taking adequate technical and organisational measures in application of the Electronic Communications Act (ECA) is punished with a fine between 400 EUR and 400,000 EUR (articles 114 and 145).

1.2 Do any of the above-mentioned offences have extraterritorial application?

Usually, there is no extraterritorial application of Belgian laws.

Article 3 BCC provides that the criminal courts shall be competent for all crimes in Belgian territory. To localise a criminal offence, Belgium applies the ubiquity doctrine, which provides that a criminal offence is situated in all places where there is a constitutive element to the offence.

This theory is supplemented with the principle of indivisibility, which allows courts to take into consideration all elements that are indivisibly connected with a criminal offence located in Belgium and to declare itself competent with regards to a co-perpetrator located in a foreign country.

In the context of specific criminal offences, the Belgian criminal law provisions apply extraterritorially, e.g. in case of terrorism. The GDPR applies extraterritorially by the criteria in article 3.2.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

A court may consider mitigating circumstances, such as the behaviour of the perpetrator in determining the criminal sanctions or giving suspension/postponement of punishment. A pro-active notification or a declaration or plea of guilt may induce a court to impose lower penalties. An amicable settlement with the Public Prosecutor can also be possible.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

When a denial-of-service attack or an infection of IT systems (article 550*ter* BCC) concerns a terrorism offence, the term of imprisonment increases by up to five years (article 137, §2,4°/1 and article 138, §1,4° BCC).

Denial-of-service-attacks could also be qualified as stalking, in application of article 442*bis* BCC, when the offender knew or should have known that his behaviour would seriously disturb the peace of that attacked person. The penalties are between 15 days and three years of imprisonment and/or a fine between 400 EUR and 2,400 EUR.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Cybersecurity:
- Act of 1 July 2011 on the security and protection of critical infrastructures.
- Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- Act of 7 April 2019 establishing a framework for the security of network and information systems of general interest for public security.
- Royal Decree of 12 July 2019, implementing the law of 7 April 2019, establishing a framework for the security of network and information systems of general interest for public security and the law of 1 July 2011 on the security and protection of critical infrastructures.
- Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity), information and communications technology, cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems, and of the parameters for determining whether an Incident has a substantial impact.

Cybercrime:
- Belgian Criminal Code, as amended by the Act of 28 November 2000 on cybercrime, and the Act of 15 May 2006 on cybercrime.
- Belgian Code of Criminal Proceedings.
- Act of 13 June 2005 on electronic communications.

Data protection:
- Article 22 of the Belgian Constitution.
- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Act of 3 December 2017 establishing the Data Protection Authority.
- Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.
- Act of 5 September 2018 setting up the information security committee and amending various laws on the implementation of the General Data Protection Regulation and repealing Directive 95/46/EC.

Electronic communications, security of electronic communications and secrecy of electronic communications:
- Article 22 of the Belgian Constitution.
- Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications.
- Act of 13 June 2005 concerning electronic communications.
- Articles 259*bis* and 314*bis* of the Belgian Criminal Code.
- Coming soon: Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

Trust services and electronic signatures:
- Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93/EC ("eIDAS Regulation").
- Title 2 of Book XII of the Belgian Code of Economic Law.
- Act of 18 July 2017 on electronic identification.
- Act of 20 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier and the elimination of obstacles to the conclusion of contracts by electronic means.
- Royal Decree of 25 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier.

Intellectual property rights:
- Book XI of the Belgian Code of Economic Law.

Employee surveillance and BYOD:
- Article 22 of the Belgian Constitution.
- General Data Protection Regulation.
- Act of 13 June 2005 concerning electronic communications.
- Articles 259*bis* and 314*bis* of the Criminal Code.
- Collective Bargaining Agreement No. 68 on employee camera surveillance.
- Collective Bargaining Agreement No. 81 on the protection of employees in relation to the surveillance of electronic online communication data.

Professional secrecy:
- Article 458 of the Belgian Criminal Code.
- Act of 30 July 2018 on the protection of trade secrets.

Due diligence and due care:
- Articles 1382 and 1383 of the Belgian Civil Code.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Critical infrastructures are governed by the Critical Infrastructures Act (CIA). The personal scope of this Act is larger than that of Directive 2008/114/EC, which it implements in Belgian law. The CIA not only covers the energy and transportation sectors, but also the financial and electronic communications sectors.

There are no specific cybersecurity provisions in the CIA. It applies to all risks that may disrupt or destroy critical infrastructures, including cyber risks. Critical infrastructures must establish and execute a security plan, which may include cybersecurity measures.

The Belgian Cyber Security Act of 7 April 2019 (CSA) implements the NIS-Directive. This Act does not directly exceed the NIS-Directive, but provides a wide range of powers and means for the implementation, monitoring and sanctioning of obligations under the NIS-Directive, e.g., security plans, annual internal audits, triennial external audits and administrative and criminal sanctions.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Operators of essential services must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations, e.g., security plan, annual internal audit, triennial external audit, etc. (articles 20–23 CSA).

Digital service providers must identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of their network and information systems. They shall take into account the following elements: (a) the security of systems and facilities; (b) Incident handling; (c) business continuity management; (d) monitoring, auditing and testing; and (e) compliance with international standards (articles 33–34 CSA).

Critical infrastructures must establish and implement a security plan (B.P.E.) (article 13 CIA). This obligation implicitly includes Incident prevention and handling.

Providers of electronic communications services or electronic communications networks must implement adequate measures to manage the security risks in relation to their services or networks, including measures to mitigate the impact of security Incidents in relation to the end-users and other connected networks (article 114, §1 ECA).

Taking into account the state of the art, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide (article 19 eIDAS Regulation).

The general principle of due diligence and due care will, in all likelihood, induce organisations to implement measures to prevent and handle Incidents in order to avoid or limit claims for damages. It does not, however, explicitly impose Incident prevention and handling.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Conflict of laws issues almost invariably arise. The measures to monitor, detect, prevent or mitigate Incidents must always be implemented in a manner that complies with the Applicable Laws, which are:

- GDPR if personal data is being processed.
- Article 124 ECA and article 314*bis* BCC if electronic communications are involved.
- Collective Bargaining Agreement No. 68 (camera surveillance) and No. 81 (surveillance of online communications) concerning the surveillance of employees.

CSA provides a settlement, stipulating that it does not affect the application of, amongst others, the GDPR, CIA, articles 259*bis*, 314*bis*, 380, 382*quinquies*, 383*bis*, 383*bis*/1, 433*septies*, 433*novies*/1, 458*bis*, 550*bis* and 550*ter* BCC.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Operators of essential services report immediately all Incidents that have a significant impact on the availability, confidentiality, integrity or authenticity of the network and information systems on which the essential service or services it provides depend on. This notification is simultaneously made to the national CSIRT, the sectoral government, or its sectoral CSIRT, and the Directorate General Crisis Centre of the Ministry of Interior Affairs.

The notification is required even if the operator only has partial access to the relevant information to determine whether the Incident has a significant impact (articles 24–25 CSA).

Digital service providers have the same duty for the services offered by them in the European Union. The notification is made in accordance with the implementing Regulation 2018/151 of 30 January 2018 on a secured platform (articles 35–36 CSA).

The controller under the GDPR shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Belgian Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification must include the following information:

- the nature of the personal data breach;
- contact details of the DPO or other contact point;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken.

Providers of electronic communications services/networks are subject to a binding personal data breach notification with the Belgian Data Protection Authority and, if impacted, the end-user, unless the provider has implemented mitigation measures (article 114/1, §3 ECA). They also have to notify the Belgian Institute for Post and Telecommunications and the end-users about special security risks (article 114/1, §1 ECA). Security Incidents also have to be notified to the Belgian Institute for Post and Telecommunications (article 114/1, §2 ECA).

Trust service providers must notify the Belgian Ministry of Economic Affairs or the Data Protection Authority about any breach of security or loss of integrity that has a significant impact on the trust service (article 19 eIDAS Regulation).

Critical infrastructures must notify any Incident that imperils the security of the critical infrastructure to the Communication and Information Centre (article 14, §1 CIA).

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations are normally permitted to voluntarily share information related to (potential) Incidents. Limitations may apply as a result of contractual confidentiality obligations or privacy and data protection laws.

Critical infrastructures are subject to a specific obligation of professional secrecy in relation to their designation, information communicated to them by various public authorities and the contents of the security plan (article 23 CIA). A breach of this obligation is a criminal offence pursuant to article 458 BCC. This secrecy obligation is sufficiently narrow to enable critical infrastructures to share information about (potential) Incidents.

Potential operators of essential services are allowed to report Incidents on a voluntary basis that have significant consequences for the continuity of the services they provide in Belgium (article 30 CSA).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Article 34 GDPR: When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate this breach to the data subject without undue delay. The information provided must, at least, include contact details of the DPO, likely consequences and measures taken or to be taken.

Article 114/1, §1 ECA: If there is a particular risk of network security breaches, the undertakings providing a publicly available electronic communications service shall inform subscribers and the Institute. If the risk requires measures other than those that can be taken by the undertakings providing the service, they shall indicate any means of combating that risk, including an indication of the expected costs.

Article 19 eIDAS Regulation: When it is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall notify the natural or legal person of the breach of security or loss of integrity without undue delay.

The nature and scope of information is different for each notification duty.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, it is understood, however, that where personal data is involved, the sharing of information will have to be organised in such a manner as to comply with the GDPR.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The following regulators are responsible for enforcement (excluding criminal actions):

- Data protection: the Belgian Data Protection Authority.
- Electronic communications: the Belgian Institute for Post and Telecommunications.
- Trust services: the Ministry of Economic Affairs.
- Critical infrastructures: the Ministry of Interior Affairs.
- Operators of essential services and digital service providers: Centre for Cybersecurity Belgium (CCB), the Ministry of Economic Affairs and sectoral governments.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The following penalties apply:

- Data protection: criminal penalties (indirectly to subsequent failures article 226 Belgian GDPR Act) and administrative penalties (article 83, §4 GDPR).
- Electronic communications: criminal penalties (articles 114 and 145 Electronic Communications Act).
- Critical infrastructures: criminal penalties (article 26 Critical Infrastructures Act).
- Operators of essential services and digital service providers: criminal and administrative penalties (articles 51 and 52 Belgian Cyber Security Act).

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No specific information on enforcement is already available. Only that of the Belgian Data Protection Authority imposing an administrative fine of 2,000 EUR for the illegitimate processing of personal data in the context of the elections.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
This is not explicitly forbidden. Only when the IP address is considered to be personal data under the GDPR that the processing has to be compliant with the GDPR. An informed consent can be required in that case. Beacons, fingerprints and cookies also require informed consent under the ECA if they are not merely functional and/or collect personal data.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
This is not explicitly forbidden.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
This is not explicitly forbidden.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice in relation to Incident handling varies greatly depending on the sector and nature of the activities.

Typically, the financial sector has implemented strict information security measures.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The telecommunications sector is subject to specific obligations under the ECA (article 114/1).

Although these are technically not legal requirements, the financial services sector is subject to specific cybersecurity obligations in the context of the prudential supervision by the National Bank of Belgium.

In addition to this, the financial services sector and the telecommunications sector are governed by the CIA, which imposes security obligations.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

A director may be held liable for a breach of his duties as a director if he fails to act with due care and due diligence.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no specific obligation to designate a CISO as such. Under the GDPR, it can be required to designate a DPO (article 37 GDPR). Operators of essential services and digital service providers are obliged to designate a contact point for the security of network and information systems (articles 23 and 34 CSA). The same obligation applies to Critical Infrastructures (articles 12 and 13 CIA).

(b) A written response plan or policy is required under articles 20 and 21 (Operators of essential services) and article 33, §1, b) (Digital service providers) CSA.
Article 13 CIA requires that the operator is responsible for organising exercises and for updating the security plan.
It may be required under the GDPR, depending on the company's individual context. This is the case under article 35, §7, d) GDPR when a data protection impact assessment is needed and may also be required as a general but implicit security measure under article 32 GDPR.

(c) CSA explicitly requires an annual internal audit and a triennial external audit for operators of essential services (article 38, §1 and 2). Article 13, §6 CIA: The operator is responsible for organising exercises and for updating the B.P.E., based on the lessons learned from the exercises or from any change to the risk analysis. It may be required under the GDPR, depending on the company's individual context.

(d) *Idem* as (c).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Besides the abovementioned notification duties, there are no specific disclosure requirements for companies in relation to cybersecurity risks or Incidents. If cybersecurity risks or Incidents have a major financial impact, there is a disclosure requirement in relation to the financial impact (e.g. in the annual report). If they have an impact on personal data, there is a disclosure obligation to the DPA.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Companies under application of the CSA are required to cooperate in controls and the supervision of the inspection. If not, criminal and administrative penalties are provided.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the case of negligence, any person suffering damage may file an action to obtain compensation. That person is required to adduce evidence of the existence of negligence (which may be adduced by evidencing a breach of Applicable Laws), the damages suffered and the causal link between the negligence and the damage.

If the Incident is the result of an unfair market practice or a breach of data protection law, cease-and-desist proceedings are possible.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Although there have been several Incidents, there have recently been no noteworthy cases in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes, see question 5.1.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber insurance is permitted and even encouraged in Belgium.

The number of Incidents has even led to a greater general awareness and demand for insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are generally no legal or regulatory limitations in relation to insurance coverage, except the possibility for insurance against criminal penalties. Administrative fines may, however, be covered by insurance.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The monitoring of employees must be done in a manner that is compliant with the principle of privacy in the work space, which includes compliance with:

- The GDPR, if personal data is being processed.
- The secrecy of electronic communications (article 124 ECA and the Collective Bargaining Agreement No. 81).
- In case of employee surveillance by cameras, Collective Bargaining Agreement No. 68.

Article 17 of the Act of 3 July 1978 on employment contracts imposes an obligation on the employee to work carefully, honestly and accurately. This may be construed as a good faith obligation to disclose risks, flaws and Incidents to the employer, although this conduct is usually described in a more explicit security policy.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Not generally, but whistle-blowing and reporting must be organised in a manner that is compliant with data protection laws.

Employees are bound by a confidentiality obligation in relation to know-how, trade secrets and personal and confidential matters (article 17, §3 of the Act concerning employment contracts), which may limit the possibility for an employee to report to third parties the existence of risks, flaws or (potential) Incidents.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have a variety of investigatory powers at their disposal, including:

- conducting (international) network searches;
- the right to copy, block or seize electronic data;
- intercepting, localising and accessing electronic communications;
- imposing technical cooperation from persons with knowledge about the relevant IT systems; and
- under very specific circumstances, hacking and computer sabotage, as well as decryption.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Organisations are not required to implement backdoors. However, law enforcement authorities may require any person with the relevant knowledge to provide them with encryption keys.

Roeland Lembrechts is a Master of Criminology (2005) and Master of Law (2009). He started his career in 2009 at the Bar of Mechelen with a broad focus on criminal, civil and corporate law, and specialised on contractual and non-contractual liabilities.
In addition, Roeland is active as a board member of the department of contract law at the Bar of Antwerp and is secretary of the professional journal '*Today's Lawyer*', a magazine that focuses on the lawyer as an ethical and innovative entrepreneur with a focus on digitising the profession.
Roeland has a special interest in contract and liability law within the digital single market.
He is a certified DPO since 2017.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: roeland@siriuslegal.be
URL: www.siriuslegal.be

Bart Van den Brande has been a member of the Dutch-speaking Brussels Bar Association since 2001.
Bart has worked at several well-known Brussels law firms and has built extensive expertise in media and advertisement law, market practices and consumer protection, intellectual property, internet and e-commerce, privacy and data protection, IT, software development and gambling law.
Parallel to his law practice, Bart was a part-time teaching assistant at Brussels University VUB between 2005 and 2013. He is the author of several articles, is an experienced speaker in seminars and for training courses and is regularly asked to comment on current legal events in the national media. Several court cases handled by Bart were later published.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: bart@siriuslegal.be
URL: www.siriuslegal.be

Sirius Legal is a Belgian boutique law firm specialising in internet law, advertisement law, media and entertainment law, IP/IT, consumer protection, gambling and cybersecurity. The Sirius Legal team is a small and young but experienced team of law professionals that try to offer tailor-made solutions to a wide range of clients, ranging from multinationals to individual players.

www.siriuslegal.be

SIRIUS.LEGAL
BUSINESS LAW FIRM

Brazil


Daniel Pitanga Bastos De Souza


João Daniel Rassi

Siqueira Castro – Advogados

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking constitutes a criminal offence in Brazil under Law No. 12.737/2012. This Law modified Provision 154-A of the Brazilian Criminal Code to provide that the invasion of a third party's computing device, whether or not it is connected to a computer network, through undue violation of a security mechanism and with the purpose of obtaining, adulterating or destroying data is a crime in Brazil. The maximum penalty for such an offence is one year of imprisonment and a fine, or two years of imprisonment and a fine if the hacker obtains the victim's private electronic communications contents, commercial or industrial secrets, or sensitive information. The two years of imprisonment and a fine also apply if the hacker controls the invaded device remotely. The aforementioned penalties may be increased where there are aggravating circumstances.

Denial-of-service attacks
Denial-of-service attacks can be punished under the Brazilian Criminal Code. According to Provision 266, the interruption or disturbance of telegraph, radiotelegraph or telephone services as well as telematics services or public utility information services shall be punished with imprisonment and a fine. The maximum penalty is three years of imprisonment, and this penalty may be doubled if the offence occurs during a public calamity.

Phishing
There is no specific provision regulating phishing in Brazil.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware is a criminal offence in Brazil. According to Provision 154-A of the Brazilian Criminal Code (modified by Law No. 12.737/2012), the installation of vulnerabilities in a third party's computing device, whether or not it is connected to a computer network, to obtain an illicit advantage shall be punished with up to one year of imprisonment and a fine. The penalty may be increased where there are aggravating circumstances.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
There is no specific provision regulating possession or use of hardware, software or other tools used to commit cybercrime in Brazil. However, the production, offering, distribution, selling or sending of a computer program or device to allow the invasion of a third party's computing device, whether or not it is connected to a computer network, through undue violation of a security mechanism and with the purpose of obtaining, adulterating or destroying data constitutes a crime punishable with up to one year of imprisonment and a fine.

Identity theft or identity fraud (e.g. in connection with access devices)
There is no specific provision regulating identity theft or identity fraud in connection with access devices in Brazil. Notwithstanding, identity theft or identity fraud, by any means, constitute the crime of false identity, punishable with up to two years of imprisonment or a fine. Further, other criminal provisions may apply in a specific case, such as ideological falsity.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
See the answer in respect of "Hacking" and "Infection of IT systems with malware" above. Further, breach of confidence by a current or former employee is classified as unfair competition under Law No. 9279/96 (Industrial Property Law), punishable with up to one year of imprisonment or a fine.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Unfair competition provisions stated in the Industrial Property Law may apply in some circumstances. Unfair competition is a criminal offence in Brazil punishable with up to one year of imprisonment or a fine.

Failure by an organisation to implement cybersecurity measures
Failure by an organisation to implement cybersecurity measures is not a criminal offence in Brazil.

1.2 Do any of the above-mentioned offences have extraterritorial application?

There is no specific provision regulating extraterritorial application of cybersecurity crimes in Brazil. However, as a rule, Brazilian criminal provisions may apply outside its territory in some circumstances provided by law.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There are possibilities for penalty mitigation in specific circumstances (e.g. cooperation with investigations).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

At first, any criminal offence perpetrated in a cybernetic context may be punished in the same way as it would if committed outside of such context. In this sense, a very common offence is the crime of extortion in the context of a ransomware cyber attack.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Besides criminal provisions, there are important provisions related to civil rights in Brazilian Law. Brazilian Internet Law (Law no. 12,965/2014) and its regulatory Decree (No. 8.771/2016) establish principles, warranties, rights and duties for internet use in Brazil. Industrial Property Law (Law No. 9,779/96) provides that the disclosure of confidential information in industry, commerce and services is classified as unfair competition, with civil and criminal effects. Moreover, the Brazilian Data Protection Law will come into force in August 2020, requiring that organisations implement technical measures to safeguard personal data. Furthermore, the Central Bank of Brazil issued Resolution No. 4.658/2018, which will fully come into force on 31 December 2021, concerning the adoption of measures in the field of cybersecurity.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Yes. Generally, cybersecurity requirements are provided by regulatory agencies. For instance, financial services providers, regulated by the Central Bank of Brazil, have specific rules related to cybersecurity. As mentioned above, the Central Bank of Brazil issued Resolution No. 4.658/2018, which regulates the adoption of measures in the field of cybersecurity.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Brazilian Data Protection Law, which will come into force in August 2020, organisations will be required to take security, technical and administrative measures to safeguard personal data and National Data Protection Authority (created by the Law No. 13.853/2019) will have the power to enforce the Law and punish organisations that do not comply with the related measures to monitor, detect, prevent or mitigate Incidents.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Yes. Adoption of measures to monitor, detect, prevent or mitigate Incidents may conflict with Applicable Laws and Tribunal precedents (e.g. the right of privacy of the employee in the workplace).

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. According to the Brazilian Data Protection Law, which will be in force in August 2020, controllers must inform the Data Protection Authority of any occurrence of security Incidents that may create risk or relevant damage to the personal data subjects. Controllers must detail within a reasonable period the extent of the damage and provide information about the affected data, about risks involved and all the technical and security measures taken in order to solve the problem or mitigate its effects. Controllers will not be responsible for security Incidents if they prove that there has been no violation of Data Protection Law or that the damage is due to the sole fault of the personal data holder.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

According to the Data Protection Law, security Incidents that may cause risk or damage to data subjects must be reported to the National Data Protection Authority and to the data subject. In

particular cases, the Authority may order the Controller to report the Incident through the media.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes. According to the Brazilian Data Protection Law, which will be in force in August 2020, controllers must inform affected individuals of any occurrence of a security Incident that may create risk or cause relevant damage to them. The communication shall be carried out in a reasonable period (to be determined by the Data Protection Authority) and shall contain a description of the nature of the affected personal data, information regarding the data subjects, an indication of the adopted technical and security measures to protect the data, the risks related to the Incident, and the measures that were or will be taken to reverse or mitigate the effects of the damage. Further, in case the communication was not immediate, the controller must provide reasons for the delay.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No. Incident reports to the National Data Protection Authority and to the data subject is mandatory anyway.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Brazilian Data Protection Law empowers the National Data Protection Authority as the only regulator of data protection in Brazil. According to the Law, the Authority will, among other prerogatives, ensure the protection of personal data, apply sanctions to controllers and processors which fail to comply with the Law, promote studies and international cooperation with authorities in other countries and edit regulations and procedures concerning privacy and personal data.

In addition, other regulators may supervise compliance with sector regulations and standards (e.g. the Central Bank of Brazil may supervise the compliance of financial institutions with its Resolution No. 4.658/2018).

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The Brazilian Data Protection Law provides penalties for infringements, including: a warning, indicating the deadline for the adoption of corrective measures; a single fine of up to 2% of the company's, group's or conglomerate's revenues in Brazil in its last fiscal year, excluding taxes, up to R$ 50,000,000.00 per infraction; a daily fine; publication of the infraction after it has been duly verified and its occurrence is confirmed; blockage of the personal data to which the infraction relates, until regularisation thereof; and elimination of the personal data to which the infringement relates.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The Data Protection Law will come into force only in August 2020, so there are no examples of enforcement in terms of this Law. However, Public Prosecutors and Consumer Protection Organizations are already acting to protect personal data, as we will see in question 8.1.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The Data Protection Law provides that controllers will have to take technical security measures to protect personal data of non-authorised access, but does not specify such measures. When the National Data Protection Authority starts its operation, regulations will be edited in order to specify what companies must do and also what they cannot do concerning data protection.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
We believe that specific security measures will be listed in future regulatory acts from the Data Protection Authority.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There is nothing specific about this security measure, but it may be regulated by the National Authority.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Under the Brazilian Data Protection Law, all companies must comply with this law and provide security measures. The Law does not distinguish business sectors. Banks and financial companies are usually more committed to information security because of the risks involved in their business (e.g. identity theft and identity fraud are widely perpetrated in Brazil).

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Besides the Brazilian Data Protection Law, which widely regulates data protection, the Brazilian Central Bank issued an act on cybersecurity policy and the contracting of data processing and storage and cloud computing to be observed by financial institutions and other institutions regulated by the Central Bank (Resolution No. 4.658/2018).

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

A breach of directors' duties would arise if the failure happens due to a director's action that is not compliant with the law or with the company's bylaws.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Brazilian Data Protection Law determines that controllers shall appoint a Data Protection Officer, who will be in charge of communications with the Data Protection Authority and data subjects, as well as of controllers' compliance. The Data Protection Law does not oblige the controller to create an Incident response plan, conduct periodic cyber risk assessments or perform penetration tests or vulnerability assessments, but the adoption of such measures may mitigate possible penalties. Moreover, the Data Protection Authority may regulate those matters in the future.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Yes. The Brazilian Data Protection Law provides that controllers must inform the Data Protection Authority and data holders of any occurrence of a security Incident that may create risk or relevant damage to the data subject.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Brazilian Data Protection Law provides that processing agents (controllers and processors) shall adopt security, technical and administrative measures to protect personal data from unauthorised access and accidental or unlawful situations of loss, alteration, destruction, communication or any improper or unlawful processing of data. Such measures shall be complied with by processing agents from conception through to the execution of the product or service.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The civil actions that may be brought depend on the nature of the Incident, but in general, Incidents involving breach of privacy, data theft, ransomware, and breach of the Brazilian Data Protection Law are dealt with by means of a tort lawsuit. Given the distribution of liability defined in the Brazilian Data Protection Law, there is also a possibility for the data processing company to be sued.

With regards to the elements that must be met in such action, it is notable that the defendant must be identified. In this sense, if the person/company responsible for the Incident is not known, the plaintiff must file a previous lawsuit against the internet service provider through which the person responsible for the Incident has operated. In this previous lawsuit, the plaintiff would need to request that the internet provider inform the IP of the party responsible for the Incident. However, in some circumstances, it may not be possible to identify the person responsible for the Incident. This is one of the main legal difficulties in dealing with cyberattacks in Brazil.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

A well-known ticket sales company was responsible for an Incident in which personal data of registered clients was exposed upon access of the company's website. The incident was caused by a security failure in the company's website and gave rise to a huge number of lawsuits.

Additionally, the Consumer Protection Authority issued a notice to the company, requesting information regarding the Incident and the measures taken to prevent such event from happening again. In this case, although there was no Data Protection Law in force in Brazil, the Consumer Protection Authority may request the adoption of measures to companies in any circumstance that involves consumers' rights. Also, the Consumer Protection Authority may apply a fine based on the Consumer Code.

Last year, the Brazilian Institute of Consumers Protection sued the subway company of São Paulo in order to prevent the collection of the passengers' facial data. The State Court of São Paulo held that the defendant should stop to collect passengers' facial data.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Brazilian law allows individuals and companies to file lawsuits claiming damages in any situation, including in relation to an incident.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no such regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no such specific requirements.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no such Applicable Laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Even before the Data Protection Law comes into force, several actions have been taken by Public Prosecutors concerning personal data protection. Prosecutors investigate several companies that deal with personal data, online payment companies, social media companies, telephone companies, hotels networks and even drug-stores. A famous online shoe store, through an agreement with Prosecutors, agreed to pay R$ 500,000.00 as indemnity for violation of personal data security.

As we mentioned earlier, the State Court of São Paulo ordered the cessation of the procedure of facial data collection by the subway company, after a lawsuit filed by the Brazilian Institute of Consumers Protection.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements.

Daniel Pitanga Bastos de Souza graduated from the Catholic University of Salvador in 2006. He obtained a postgraduate degree in intellectual property law from the Catholic University of Rio de Janeiro and specialised in entertainment law at the State University of Rio de Janeiro. He also holds an LL.M. in information technology and telecommunications law from the University of Southampton. He is a member of the Brazilian Bar Association, Rio de Janeiro section and Chair of the Anti-Piracy Committee at the Brazilian Bar Association, Rio de Janeiro section. He is the Co-Chair of the Interactive Entertainment and Media Committee at the International Technology Law Association (ITechLaw).

Siqueira Castro – Advogados
Praça Pio X, 15, 3º andar
Rio de Janeiro – RJ
Brazil

Tel: +55 21 2514 7496
Email: dpitanga@siqueiracastro.com.br
URL: www.siqueiracastro.com.br

João Daniel Rassi is the head partner of the Business Crime Department of Siqueira Castro Advogados. He holds a specialisation in criminal law at Salamanca University, Spain, has received a Master's degree in criminal law from University of São Paulo (USP) and has a PhD in both criminal law and criminal procedure law from USP.
Throughout more than 20 years working as a criminal lawyer, Mr. Rassi has participated as defence counsel in a series of media cases, in areas connected to business activities, such as criminal proceedings involving corruption, money laundering, environmental offences, the tax and fiscal system, the financial and capital markets, intellectual property, antitrust and consumer relations, as well as combatting corporate fraud and assessing compliance programmes. His professional experience includes negotiations of successfully concluded collaboration agreements with the Brazilian Office of Prosecutor General.
Mr. Rassi has been listed by *Chambers and Partners*, *Latin Lawyers* and *Análise Advocacia* as one of the most respected lawyers in Brazil and Latin America in the area of criminal law and dispute resolution regarding white-collar crimes.

Siqueira Castro – Advogados
Rua Tabapuã
No. 81, 4th Floor – Itaim Bibi
São Paulo
Brazil

Tel: +55 11 3704 9840 / 3594 0900
Fax: +55 11 3704 9848
Email: rassi@siqueiracastro.com.br
URL: www.siqueiracastro.com.br

Canada


Lyndsay A. Wasser


Kristen Pennington

McMillan

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Wilful interception of private communications is a criminal offence under Section 184 of the Canadian Criminal Code, RSC 1985, c C-46 (the "**Code**"), with a maximum sentence of five years' imprisonment.

Section 342.1 of the Code prohibits fraudulently obtaining any computer service or intercepting any function of a computer system. Use of a computer system with intent to commit such an offence and use or possession of a computer password to enable such an offence are also prohibited. The maximum sentence is 10 years' imprisonment.

Hacking has also been prosecuted under:

- Section 380(1) of the Code, which prohibits defrauding the public or any person of property, money, valuable security or a service. In *R v. Kalonji*, the accused was found guilty of fraud and conspiracy to commit fraud in connection with an account take-over scheme involving hacking bank accounts.
- Section 430 of the Code (see below), particularly when the hacking is related to "smurfing" (i.e., overloading computer systems causing chaos). In *R v. Geller*, an accused was charged with mischief to data after obtaining credit card numbers and other information through hacking, then accessing the internet using fake identification.

Denial-of-service attacks
Denial-of-service attacks could be considered "mischief" under Section 430(1.1) of the Code, which includes obstructing, interrupting or interfering with the lawful use of computer data and denying access to computer data to a person who is entitled to such access. The maximum penalty is 10 years' imprisonment.

Phishing
Phishing constitutes fraud pursuant to Section 380(1) of the Code. In *R v. Usifoh*, the accused was found guilty of receiving funds from various victims of phishing scams.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Section 430 of the Code prohibits "mischief", which includes wilfully destroying/damaging property, rendering property useless/inoperative/ineffective or obstructing/interrupting/interfering with the lawful use, enjoyment or operation of property. Section 430(1.1) specifically prohibits wilfully destroying or altering computer data, rendering computer data meaningless, useless or ineffective, obstructing, interrupting or interfering with the lawful use of computer data and denying access to computer data to a person who is entitled to access it. The maximum penalty is 10 years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Under Section 342.2 of the Code, it is illegal to make, possess, sell, offer for sale, import, obtain for use, distribute or make available a device that is designed or adapted primarily to commit an offence under Section 342.1 (hacking) or Section 430 (mischief), knowing that the device has been used or is intended to be used to commit such an offence. The maximum penalty is up to two years' imprisonment and/or an order to forfeit the offending device(s).

Identity theft or identity fraud (e.g. in connection with access devices)
Section 402.2 of the Code prohibits obtaining or possessing another person's identity information with the intent to use it to commit an indictable offence such as fraud. The maximum sentence is five years' imprisonment. In *R v. Bigcharles*, the accused pled guilty to creating fake credit cards using personal information obtained from compromised computer systems.

Fraudulently "personating" another with the intent of gaining an advantage, obtaining property, causing disadvantage to another or to avoid arrest or prosecution is prohibited under Section 403 of the Code. The maximum penalty is 10 years' imprisonment. Personating includes pretending to be the person or using the person's identity information, including name, signature, user name or password.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Section 41.1(1) of the Copyright Act, RSC 1985, c C-42 prohibits circumvention of a "technological protection measure", including any technology, device or component that controls access to a work or sound recording or restricts violations of certain copyright provisions.

Circumventing a technological protection measure includes descrambling a scrambled work, decrypting an encrypted work or otherwise avoiding, bypassing, removing, deactivating or impairing the technological protection measure without consent.

Some violations of Section 41 can lead to fines of up to $1 million, imprisonment for up to five years or both.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Under Section 83.2 of the Code, an individual who commits an indictable offence for the benefit of, at the direction of, or in

association with an organisation that commits a terrorist activity is liable to imprisonment for life. Section 83.01 of the Code defines a "terrorist activity" to include an act or omission that intentionally causes serious interference with or disruption of an essential service, facility or system, whether public or private, other than in non-violent protests.

Failure by an organisation to implement cybersecurity measures

It is not a criminal offence for an organisation to fail to implement cybersecurity measures. However, organisations would be required to implement such measures under some of the Applicable Laws discussed below and may also face civil or regulatory liability for failing to do so.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Section 6(2) of the Code provides that "no person shall be convicted of an offence that takes place outside of Canada" (see also Section 478(1) of the Code). However, under Sections 7(3.74) and 7(3.75) of the Code, certain terrorism offences and indictable offences that are considered terrorist activities may be deemed to have been committed in Canada, including when the offence is committed by or against a Canadian citizen.

The Supreme Court of Canada has held that, where a "significant portion" of the activities constituting an offence took place in Canada, a Canadian court may assume jurisdiction. A court will consider whether there is a "real and substantial link" between the alleged crime and the jurisdiction seeking to enforce the law.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Certain criminal offences require proof of criminal intent (e.g. *mens rea*). Also, some offences may not apply where the action was undertaken with consent.

The penalties for some offences depend upon the financial repercussions of the offence. For example, Section 380(1) of the Code (see Section 1.1) carries a maximum sentence of 14 years' imprisonment for fraud involving $5,000 or more, whereas the maximum sentence is reduced to two years' imprisonment if the value of the subject-matter of the offence is less than $5,000.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The Code defines "terrorist activity" to include an act or omission that intentionally causes certain forms of serious harm, which is undertaken for political, religious or ideological purposes and is intended to intimidate the public with respect to its security, including its economic security, or to compel a person, government or organisation (whether inside or outside Canada) from doing or refraining to do any act.

Some of the offences outlined in question 1.1 are indictable offences. To the extent they constitute a terrorist activity or are committed in connection with a terrorist group, the terrorism provisions of the Code may apply.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23 ("**CASL**") prohibits: (a) alteration of the transmission data in an electronic message so that the message is delivered somewhere other than, or in addition to, the destination specified by the sender (Section 7(1)); (b) installation of a computer program on another's computer system in the course of a commercial activity without consent (Section 8(1)); and (c) aiding, inducing, procuring or causing any of the above (Section 9). Violations of CASL can result in administrative monetary penalties of up to $1 million per violation by an individual and $10 million per violation by an organisation.

Canada also has a number of statutes that apply to the protection of personal information ("**PI**"), including (collectively "**Data Protection Statutes**"):

- The Federal Personal Information Protection and Electronic Documents Act, SC 2000, c 5 ("**PIPEDA**") applies to the protection of employee PI by federally regulated organisations and all PI handled in the course of commercial activities (except in provinces that have substantially similar legislation);
- Alberta, British Columbia and Quebec each have legislation that is substantially similar to PIPEDA, which applies to the protection of PI by private sector organisations within these provinces;
- each Canadian jurisdiction has legislation governing the protection of PI by government bodies/institutions; and
- most provinces have legislation that applies to the protection of personal health information by certain types of custodians, such as doctors and hospitals.

Export control laws can also have some cybersecurity implications. For example, Canada's Export Control List (the "**ECL**") identifies specific goods and technologies that are controlled for export, including some computer systems, equipment, components and software designed or modified for the generation, command and control or delivery of "intrusion software", as defined in the ECL.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Communications Security Establishment ("**CSE**") is the technical authority for cybersecurity and information assurance in Canada. Its mandate includes providing advice, guidance and services to ensure the protection of computer networks and elec-

tronic information of importance to the Canadian government, including combatting foreign-based cyberattacks on critical infrastructure. The CSE establishes IT security standards, practices and directives for IT security practitioners across the federal government.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Data Protection Statutes require the protection of PI. For example, PIPEDA requires that PI be protected against loss or theft, unauthorised access, disclosure, copying, use or modification. The nature of the safeguards should vary depending on the sensitivity, amount, distribution, format and method of storage of the PI, and should include technological measures such as passwords and encryption.

Some of the Data Protection Statutes contain breach reporting, recording and notification obligations in the event of an Incident that impacts PI, as described further in question 2.5.

Certain industry regulators also require organisations to monitor, detect, prevent and/or mitigate Incidents, including:

- The Canadian Securities Administrators ("**CSA**") has issued several Staff Notices relevant to cybersecurity, including without limitation: Staff Notice 11-326 ("Cyber Security"); Staff Notice 11-332 ("Cyber Security"); Staff Notice 33-321 ("Cyber Security and Social Media"); Staff Notice 11-338 ("CSA Market Disruption Coordination Plan"); and Multilateral Staff Notice 51-347. These Staff Notices address matters such as the CSA's expectations for market participants (e.g., that they adopt a cybersecurity framework that is appropriate to their size and scale) and the measures firms should take to prevent and respond to Incidents (e.g., implementing preventative practices, adequate and current staff training and a written Incident response plan). Firms are expected to conduct a cybersecurity risk assessment at least annually.
- The Office of the Superintendent of Financial Institutions ("**OSFI**") has issued several publications related to cybersecurity, including the "Cyber Security Self-Assessment Guidance" memorandum for Federally Regulated Financial Institutions ("**FRFI**"), which indicates that FRFI senior management is expected to review cyber risk management policies and practices to ensure that they remain appropriate and effective based on evolving circumstances and risks. OSFI has also published a cybersecurity self-assessment template that it encourages organisations to use and may require an organisation to complete. OSFI's "Guideline B-10" sets out expectations for FRFIs on the protection of information disclosed to service providers.
- The Investment Industry Regulatory Organization ("**IIROC**") has released a "Cybersecurity Best Practices Guide", which provides dealer members with a voluntary risk-based cybersecurity framework comprising industry standards and best practices. IIROC's "Cyber Incident Management Planning Guide" assists dealer members in preparing internal response plans for Incidents.
- The Mutual Fund Dealers Association of Canada ("**MFDA**") has released a bulletin on cybersecurity describing sources of threats and providing guidance on creating a cybersecurity framework. The MFDA actively engages with members to identify risks in their cybersecurity practices and provide recommendations for improvements, including pursuant to its Cybersecurity Assessment Program.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Some Data Protection Statutes may apply to organisations outside of Canada. For example, PIPEDA applies to foreign organisations processing PI that have a "real and substantial connection" to Canada.

Canada is a signatory to the Budapest Convention on Cybercrime, which helps countries develop national legislation regarding cybersecurity and requires consultation among signatories to determine the most appropriate jurisdiction for prosecuting certain crimes related to computer systems and data.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Some Data Protection Statutes contain breach reporting and recording obligations in the event of an Incident. For example, PIPEDA requires organisations to keep records of any Incident involving loss of unauthorised access to or unauthorised disclosure of PI due to a breach of (or failure to establish) the security safeguards required by PIPEDA. If an Incident gives rise to a real risk of significant harm to any individual(s), the Incident must be reported to the Office of the Privacy Commissioner of Canada (the "**OPC**") and the organisation must notify affected individuals and any organisation or government institution that may be able to reduce or mitigate the risk of harm. PIPEDA prescribes the minimum content for reports to the OPC, including (without limitation) a description of the Incident, timing of the Incident, the PI and the number of individuals impacted and the steps taken to mitigate/reduce the risk of harm.

Some of the provincial Data Protection Statutes also contain breach reporting and notification requirements, including private-sector legislation in Alberta and legislation applicable to personal health information custodians in Ontario.

The CSA requires organisations to consider disclosure of cybercrime risks, Incidents and related controls in their prospectus or continuous disclosure filings (see question 4.3). Factors relevant to assessing disclosure obligations include the probability that an Incident will occur and the anticipated magnitude of its effects. The issuer is expected to provide disclosure that is detailed and entity-specific. In addition, regulated exchanges, marketplaces, clearing agencies and alternative trading systems may be subject to Incident reporting requirements under recognition or exemption orders issued by various CSA jurisdictions, including those set out in Instruments NI 21-101, NI 23-101 and NI 24-102. Many exchanges, marketplaces and clearing agencies are required to promptly notify

the CSA of a material systems issue, security breach or system intrusion. The CSA also expects that systematically important clearing agencies and settlement systems will inform the Bank of Canada of a market disruption event.

OSFI's "Technology and Cyber Security Incident Reporting" memorandum requires that an Incident be reported to OSFI when it could materially impact the normal operations of a FRFI (including the confidentiality, integrity or availability of its systems and information) and is assessed to be of a high or critical severity level. The memorandum lists characteristics of reportable Incidents and requires reporting to OSFI (including certain specified information) as soon as possible, but no later than 72 hours after it is determined that the Incident is reportable. FRFIs have an ongoing obligation to provide updates to OSFI as new information becomes available.

IIROC has proposed amending its Dealer Member Rules to require mandatory reporting of Incidents and, in the interim, recommends voluntary reporting.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Sharing of potential or actual Incidents is generally permitted, provided the disclosing organisation complies with all Applicable Laws (for example, abiding by any statutory or contractual confidentiality requirements and not misusing or disclosing PI contrary to Applicable Laws).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Some of the Data Protection Statutes contain notification obligations in the event of an Incident that impacts PI. For example, PIPEDA requires that individuals be notified of any breach of security safeguards involving PI under the organisation's control, as soon as feasible, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

PIPEDA prescribes the content and manner of delivering the notice. The notice must contain sufficient information to allow the individual to understand the significance of the Incident to them and to take steps to reduce/mitigate the risk of harm, and must contain certain prescribed content, including (without limitation) a description of the Incident, timing of the Incident, the PI impacted and the steps taken by the organisation to mitigate/reduce the risk of harm.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

As indicated in question 2.6, information-sharing may be restricted by Applicable Laws and contracts, including under the Data Protection Statutes (applicable to disclosing PI, including IP addresses and/or email addresses that constitute PI) and under the Competition Act, RSC 1985, c C-34 (applicable to sharing price-sensitive information). However, some Data Protection Statutes allow for disclosure of PI in certain circumstances related to the detection or prevention of unlawful activity.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Compliance with PIPEDA is generally enforced by the OPC, however, certain offences can be prosecuted by the Attorney General (the "**AG**"). Each province has a regulator responsible for enforcing the relevant provincial Data Protection Statutes.

CASL is enforced by the Canadian Radio-television and Telecommunications Commission (the "**CRTC**"), the OPC and the Competition Bureau.

See, also, the industry-specific regulators described in question 2.3, which oversee compliance with their cybersecurity policies, guidelines and industry-specific Applicable Laws.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The OPC can make non-binding recommendations in the event of non-compliance with PIPEDA and, following the OPC's decision, an application can be made to the Federal Court for damages to complainants. The AG can prosecute an organisation for failure to comply with the breach reporting, notification and recording obligations under PIPEDA, which can result in fines of up to $10,000 on summary conviction or $100,000 for an indictable offence. Some of the provincial Data Protection Statutes also provide for fines in the event of non-compliance.

Criminal offences and failure to comply with CASL carry penalties as described above.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The OPC has investigated a number of Incidents involving the breach of PI, including:

- PIPEDA Report of Findings #2016-005 – Investigation of Ashley Madison in connection with hacking and online posting of users' account information (resulted in recommendations by the OPC);
- PIPEDA Report of Findings #2019-001 – Investigation into Equifax after an attacker accessed sensitive PI of customers (resulted in a compliance agreement);

- PIPEDA Report of Findings #2018-001 – Investigation into VTech Holdings Limited following the potential compromise of PI respecting over 553,000 Canadians, including children's names, genders, dates of birth, pictures, voice recordings and chat discussions with parents; and
- PIPEDA Report of Findings #2007-389 – Investigation into TJX after a network computer intrusion affected payment card information.

The CRTC has also taken enforcement action under CASL, including against Datablocks Inc. (fine of $100,000) and Sunlight Media Network Inc. (fine of $150,000) for violations of Sections 8 and 9 of CASL. The CRTC found that advertisements distributed through the companies' services resulted in the unlawful installation of malicious programs on computer systems by third parties, and that neither company took appropriate steps to prevent such CASL breaches, thereby aiding the violations.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Organisations subject to Data Protection Statutes are generally required to provide notice and/or obtain consent to the collection and use of PI. The OPC considers metadata collected using beacons to be PI and has indicated that organisations should not undertake types of web tracking that individuals cannot stop or control without taking extraordinary measures (or at all), as these forms of tracking do not allow for individuals to consent or withdraw consent, contrary to PIPEDA.

It is possible that beacons used only for data security purposes may fall within the exceptions to notification and/or consent requirements under the applicable Data Protection Statute(s). However, a specific evaluation of Applicable Laws in the relevant jurisdiction(s) should be undertaken.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
The use of honeypots is not expressly prohibited by Applicable Laws. However, to the extent the honeypot involves the collection, use or disclosure of PI, notice and consent considerations may apply. Honeypots may be problematic under CASL, depending upon the manner in which they operate.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is not expressly prohibited by Applicable Laws. However, to the extent the sinkhole involves the collection, use or disclosure of PI, notice and consent considerations may apply. Compliance with CASL should also be considered.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Many organisations in various industries have recognised that compliance with statutory requirements should not be the end goal for data protection and have voluntarily committed to a higher standard. Examples include, without limitation, the telecommunications and financial services industries, as well as service providers to healthcare institutions and government institutions/bodies. Payment processors in Canada also typically comply with PCI-DSS.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Organisations in the financial services and telecommunications sectors must comply with PIPEDA, including (in many cases) with respect to employee personal information. See Section 2 for additional requirements applicable to the financial sector, including pursuant to OSFI guidance documents.

The Bank of Canada, Department of Finance and OSFI have also collaborated with G-7 partners to publish the following guidelines: (a) G-7 Fundamental Elements of Cybersecurity for the Financial Sector; (b) G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector; and (c) G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector.

The Canadian Security Telecommunications Advisory Committee has developed Security Best Practices for telecommunications service providers that supply and support Canada's telecommunications critical infrastructure. These voluntary practices include ongoing security testing, network security monitoring, Incident response capabilities and developing breach notification procedures.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Directors' personal liability with respect to Incidents has yet to be expressly considered by Canadian courts. However, directors can be held liable for breaches of fiduciary duties if they fail to: act honestly and in good faith with a view to the best interests of the company; or exercise the care, diligence and skill of a reasonably prudent person in comparable circumstances. Therefore, failure to take steps to address cybersecurity concerns of which the director was aware (and that a reasonable person would have remedied) could potentially expose the director to personal liability. A due diligence defence may apply if the director relied in good faith on statements, documents and reports created by professionals.

There may also be a risk of personal liability if directors misrepresent the organisation's cybersecurity measures, fail to disclose cybersecurity risks or Incidents in annual reporting (if applicable) or are otherwise untruthful about cybersecurity Incidents or risks.

Directors may also be held personally responsible for violations of certain statutes. For example, pursuant to Section 31 of CASL (subject to a defence of due diligence), an officer, director, agent or mandatary of a corporation may be liable if they directed, authorised, assented to, acquiesced in or participated in the commission of a violation of CASL.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Such measures may be explicitly required under specific sectoral or provincial laws. In any event, guidance documents and findings in prior cases published by the OPC and other regulators indicate that all organisations should have a written Incident response plan/policy, and should conduct periodic cyber risk and vulnerability assessments and penetration tests. Failure to do so would typically be considered non-compliant with the organisation's general obligations to protect information under the Applicable Laws.

Some Data Protection Statutes require organisations to designate a person responsible for compliance with the statute. For example, PIPEDA Schedule 1, Principle 4.1 requires designation of one or more individual(s) who are accountable for compliance with the PIPEDA principles, including those set out under Principle 4.7, "Safeguards".

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

As noted in question 2.5, some institutions are required to disclose cybersecurity risks or Incidents as part of their prospectus or ongoing disclosure obligations.

The CSA's Multilateral Staff Notice 51-347 ("Disclosure of cybersecurity risks and incidents"), a joint publication of the British Columbia Securities Commission, the Ontario Securities Commission and Quebec's *Autorité des marchés financiers*, provides that issuers must undertake a contextual analysis when determining whether and when an Incident constitutes a material fact or material change that requires disclosure in accordance with securities legislation. Issuers are expected to address in their Incident remediation plans how an Incident will be assessed to determine whether, what, when and how the Incident will be disclosed.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Some laws of general application and/or specific sectoral or provincial laws have requirements that are relevant to cybersecurity (e.g., Quebec's An Act to Establish a Legal Framework for Information Technology). Organisations should consult local counsel in the relevant jurisdiction(s) to ensure full compliance with all Applicable Laws.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

It is common for class action lawsuits to be filed in Canada following an Incident involving the breach of PI. Representative plaintiffs commonly allege negligence, intrusion upon seclusion, breach of fiduciary duty, breach of contract, breach of warranty, breach of confidence, violation of privacy, publicity given to private life/public disclosure of private facts, breach of consumer protection legislation and/or conspiracy.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Some examples of class action lawsuits filed in connection with Incidents include:

- *Kaplan v. Casino Rama*, 2019 ONSC 2025 – Alleging that Casino Rama breached its privacy policy by failing to take reasonable security measures to protect against unauthorised access to class members' personal and confidential information.
- *Lozanski v. The Home Depot Inc.*, 2016 ONSC 5447 – Regarding a payment card system hacked by criminal intruders using custom-built malware.
- *Drew v. Walmart Canada Inc.*, 2017 ONSC 3308 – Following the breach of an online photo centre operated by a third-party service provider.
- *Tucci v. Peoples Trust Company*, 2017 BCSC 1525 – Alleging breach of contract, confidence and privacy, negligence and intrusion upon seclusion or, in the alternative, unjust enrichment and waiver of tort regarding a compromised database.
- *Maksimovic v. Sony of Canada Ltd.*, 2013 CanLII 41305 – Following a cyber-attack resulting in access to account holder information.
- *Zuckerman v. Target Corporation*, 2017 QCCS 110 – Regarding a breach affecting payment card data, including name and credit/debit card number, expiration date and security code.

Class action lawsuits were also filed in connection with the Incidents experienced by Ashley Madison and Equifax (see question 2.11).

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

As indicated above, it is common in Canada for class action lawsuits to be filed following an Incident. Representative plaintiffs have alleged various torts, including negligence and privacy torts, such as intrusion upon seclusion. As none of these cases has yet proceeded to trial (although some have settled), the liability of organisations that experience an Incident is still unsettled law in Canada.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Many general commercial liability policies do not cover Incidents, but specialised cyber risk policies are available and typically tailored to an organisation's particular risk profile.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are not.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

As part of a privacy compliance program, organisations should implement employee training on Applicable Laws and the organisation's own privacy policies and procedures. Organisations are also expected to implement appropriate access controls and employee monitoring to protect against unauthorised access to, or use and disclosure of, personal and confidential information. Failure to do so may contravene the Applicable Laws, including general obligations to safeguard PI under the Data Protection Statutes.

Although not explicitly prescribed by legislation, employers should require their employees to report potential or actual Incidents and may, in some circumstances, implement disciplinary action for failing to do so. Failure to implement reporting procedures could result in non-compliance with statutory obligations, such as PIPEDA's breach recording and reporting obligations.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No. In fact, employees have protection for whistleblowing under some Applicable Laws, including under PIPEDA Sections 27 and 27.1 and Section 425 of the Code.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Canadian government has broad powers to investigate criminal activities, including terrorism offences. For example, Section 487 of the Code permits searches of computer systems, and generation and seizure of data printouts, and allows a court to order the preservation of computer data in some circumstances.

The Canadian Security Intelligence Service Act, RSC 1985, c C-23 allows the Director of Service or a designate to seek a warrant triggering broad powers to investigate a threat to Canadian security, both within and outside of Canada.

Regulators that are responsible for enforcing the Applicable Laws described in Section 2 (e.g., the OPC and the CRTC) also have broad investigatory powers. For example, the OPC can, amongst other powers: (a) summon and enforce the appearance of persons and compel them to give oral or written evidence on oath and to produce records in the same manner and to the same extent as a superior court of record; and/or (b) at any reasonable time, enter any premises (except a dwelling-house), and converse in private with any person or examine or obtain copies/extracts from records found in such premises.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are none.

Lyndsay A. Wasser is the Co-Chair of McMillan's Privacy & Data Protection Group and its Cybersecurity Group. She is a Certified Information Privacy Professional/Canada and regularly advises and assists clients on a broad range of privacy and cybersecurity issues, including advising on legal requirements related to data security, workplace privacy issues, handling personal health information and transferring personal information across borders. She assists clients to develop privacy compliance programs and data sharing agreements. She has assisted many clients with responding to privacy and data breaches involving various types of information (e.g., payment card information, patient data, employee personal information and sensitive identity information), including assisting with risk assessment, breach response strategy, notification obligations and communications with regulators. Lyndsay regularly writes and speaks on cybersecurity topics and is the co-author of *Privacy in the Workplace*, 4th ed. and the Privacy chapter in the *Ultimate Corporate Counsel Guide*.

McMillan
Brookfield Place, Suite 4400
181 Bay Street
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 7083
Email: lyndsay.wasser@mcmillan.ca
URL: www.mcmillan.ca

Kristen Pennington is an Associate Lawyer in the Toronto office of McMillan, where she practices both privacy and employment law. Kristen advises organisations with respect to legal requirements related to data security and workplace privacy issues, including employee background checks and cross-border transfers of personal information. She also assists clients with developing practical, up-to-date privacy compliance programs. Kristen regularly writes about emerging Canadian privacy topics and has been featured in a variety of leading industry publications.

McMillan
Brookfield Place, Suite 4400
181 Bay Street
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 7000
Fax: +1 416 865 7048
Email: kristen.pennington@mcmillan.ca
URL: www.mcmillan.ca

China

Susan Ning

Han Wu

King & Wood Mallesons

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Under the Criminal Law of the People's Republic of China ("Criminal Law"), cybercrimes are mainly provided in the section: "Crimes of Disturbing Public Order". Articles 285, 286, and 287 are the three major articles that directly relate to cybercrimes. Moreover, Article 253(1) indirectly relates to cybersecurity and applies to cases involving internet-related personal information infringement acts. The punishments for violating Articles 285, 286, and 287 include imprisonment, detention, and fines. For example, the offender may be sentenced for up to seven years' imprisonment for illegally obtaining data from a computer information system in serious cases. Entities may be convicted for violating Articles 285, 286, and 287, as unit crime has been provided for in all three articles.

It is worth noting that Articles 286 and 287 set up the principle that if someone uses computers (for example, through hacking, phishing or other internet-related illegal action) to commit other crimes, i.e. crimes that traditionally had no relationship with the internet, such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of state secrets, the offender shall be convicted of the crime for which the penalty is heavier.

Hacking (i.e. unauthorised access)

Pursuant to Article 285 of the *Criminal Law*, activities which involve invading a computer information system in the areas of State affairs, national defence or advanced science and technology constitute the "crime of invading a computer information system". The offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention. For activities of invading a computer information system other than those in the above areas, it may constitute a "crime of obtaining data from a computer information system and controlling a computer information system" and the offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention, or imprisonment for three to seven years in serious cases. If an entity commits those crimes, such entities shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences shall be punished accordingly.

For example, in the criminal case of "Wang's illegal obtainment of computer information system data and controlling a computer system", according to the final decision made by Fuyang Intermediate People's Court in Anhui Province in May 2018, the defendant was sentenced to three years in prison but suspended for five years and fined 8,000 yuan for illegally obtaining more than 9,000 pieces of personal information by using self-learning hacking technology.

Article 285 of the *Criminal Law* further provides that whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to a fixed-term imprisonment of no more than three years or criminal detention, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to a fixed-term imprisonment of no less than three years but not more than seven years, and be fined.

It is noteworthy that using web crawlers may be regarded as invading conduct in violation of Article 285 if a technical method were adopted to crack anti-crawling measures set by websites or to bypass identity check processes set in a computer server. This is supported by various criminal cases in China. For example, according to a verdict of the Beijing Haidian District People's Court against Shanghai Shengpin Network Technology Limited and its employees, the employees of the alleged company colluded to adopt technical measures to obtain video data stored in the server of the victim Beijing Byte Dance Technology Co., Ltd. Meanwhile, the CTO of the company instructed other employees to crack-down the anti-crawling measures set in the victim's server. During the data crawling process, the alleged company used the forged device ID to bypass the server's identity check process, and used fake User Agent and IP addresses to avoid the server's access restrictions. The court finally decided that the alleged company and its employees' conducts violated Article 285 of the *Criminal Law*. The alleged company were imposed a fine of RMB200,000 and the employees were sentenced to imprisonment together with fines.

Denial-of-service attacks

Pursuant to Article 286 of the *Criminal Law*, denial-of-service attacks could constitute the "crime of sabotaging computer information system" and more than five years' imprisonment may be given in particular serious cases.

Phishing

Phishing is usually performed to steal or otherwise acquire personal information of citizens, which is considered as the "crime of infringing a citizen's personal information" provided in Article 253(1) and up to seven years' imprisonment may be sentenced in serious cases.

For example, in the criminal case of "Zhang Dawei's infringement upon a citizen's personal information", the defendant established a phishing website to counterfeit the official website of Apple iCloud. In this way, the defendant obtained a victim's Apple ID and pass-

word and then sold them for profit. The court decided that the defendant committed the "crime of infringing a citizen's personal information" and imposed seven months' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
For intentional creation or dissemination of a computer virus or other destructive programs, including, but not limited to, ransomware, spyware, worms, trojans and viruses, which affect the normal operation of a computer information system, if serious consequences are caused, such activities constitute the "crime of sabotaging a computer information system" under Article 286 of the *Criminal Law*. The offender may be sentenced to five years' imprisonment in serious cases.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
If someone possesses or uses hardware, software or other tools to commit cybercrime prescribed in the *Criminal Law*, depending on the crime committed, the offender may be convicted in accordance with the corresponding article in the *Criminal Law*, such as the "crime of invading a computer information system". Further, if a person provides hardware, software or other tools specially used for invading or illegally controlling computer information systems, or if the person knows that any other person is committing the criminal act of invading or illegally controlling a computer information system and still provides programs or tools for such a person, he/she shall commit the crime of "providing program or tools for invading or illegally controlling computer information systems".

There is also an offence, i.e. "illegal use of information networks", which involves activities that take advantage of an information network to establish websites and communication groups for criminal activities, such as defrauding, teaching criminal methods, producing or selling prohibited items and controlled substances. If the criminal activity also constitutes another offence, the offender shall be convicted of the crime which imposes a heavier penalty.

Identity theft or identity fraud (e.g. in connection with access devices)
Under the *Criminal Law*, for identity theft, if the offender obtains identities by stealing or otherwise illegally acquires the personal information of citizens, such activity may be convicted as the "crime of infringing a citizen's personal information" pursuant to Article 253(1). If someone uses the stolen identity of others as its own proof of identity, such behaviour may constitute the "crime of identity theft" under Article 280(1) of the *Criminal Law*; in case such person uses the stolen identity to commit fraud or other criminal activities, he/she should be convicted of the crime the penalty of which is higher.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
If a current or former employee breaches confidentiality obligations and causes infringement of personal information, trade secrets, state secrets, etc., the offender will be convicted pursuant to Article 287 and punished in accordance with the relevant provisions of the *Criminal Law*, such as the "crime of infringing trade secrets".

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
If someone, in violation of laws and regulations, deletes, amends, adds or disturbs functions of a computer information system and causes the computer information system's inability to work normally or conducts operations of deletion, amendment or addition towards the data or application programs which are stored, disposed of or transmitted in a computer information system, and serious consequences are caused, such activities constitute the "crime of sabotaging computer information system" under Article 286 of the *Criminal Law*. The offender shall be sentenced to a fixed-term imprisonment of more than five years if serious consequences have incurred.

Failure by an organisation to implement cybersecurity measures
Pursuant to Article 286(1) of the *Criminal Law*, if an organisation is a network service provider, and does not perform its duties of safety management, provided by laws and administrative regulations, on its information network, and refuses to correct its conduct after the regulatory authorities order it to rectify the non-performance, the organisation shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences may be sentenced to a fixed-term imprisonment of no more than three years, under any of the following circumstances:
(1) resulting in the dissemination of a large amount of illegal information;
(2) causing the disclosure of user information, resulting in serious consequences;
(3) causing the damage or loss of criminal evidence which results in serious consequences; or
(4) other serious circumstances.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above-mentioned offences have extraterritorial application. First, if the criminal act or its consequence takes place within the territory of China, the crime shall be deemed to have been committed within the territory of China. Second, the *Criminal Law* is applicable to citizens of China who commit crimes prescribed in the *Criminal Law* outside the territory of China; however, if the maximum penalty of such crime prescribed in the *Criminal Law* is a fixed-term imprisonment of not more than three years, the offender could be exempted from punishment. Third, if a foreigner commits a crime outside the territory of China against the State or against Chinese citizens, the offender may be convicted pursuant to the *Criminal Law* if the *Criminal Law* prescribes a minimum punishment of fixed-term imprisonment of not less than three years; however, the *Criminal Law* shall not apply if it is not punishable according to the law of the place where it was committed.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

For the above-mentioned offences, there are no specific mitigation conditions prescribed in these articles. However, the mitigation conditions prescribed in the *Criminal Law* for all crimes are applicable. For example, if an offender voluntarily gives oneself up to the police and confesses his crimes or exposes others' crimes that can be verified, the offender would be given a mitigated punishment.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Article 287(2) of the Criminal Law provides for the "crime of assisting information network criminal activity", which regulates activities of providing internet access, server hosting, network storage, communication transmission and other technical support while being aware that others use such information networks to commit criminal offences (e.g. activities that lead to cybersecurity Incidents or terrorism activities).

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The *Cybersecurity Law of the People's Republic of China* ("**Cybersecurity Law**"), which came into force on 1 June 2017, is a law covering various aspects of network security and has laid the foundation for a comprehensive cybersecurity regulatory regime in China. So far, a series of specific measures aimed at facilitating the implementation of the *Cybersecurity Law* have already been enacted, such as the *Measures on the Security Review of Network Products and Services (for Trial Implementation)*, the *National Emergency Response Plan for Cybersecurity Incidents*, and the *Provisions on Protection of Children's Personal Information Online*.

The *Cybersecurity Law* recognises the graded cybersecurity protection as the basic legal system to ensure network security in China. While the *Regulation on Graded Protection of Cybersecurity* is still seeking opinions, relevant authorities have officially promulgated three recommended national standards regarding graded cybersecurity protection in May 2019 for guiding the graded protection, which will come into force on December 1, 2019. These national standards include the *Information Security Technology-Baseline for Classified Protection of Cybersecurity* (GB/T 22239-2019) which replaces GB/T 22239-2008, the *Information Security Technology-Evaluation Requirement for Classified Protection of Cybersecurity* (GB/T 28448-2019) which replaces GB/T 28448-2012, and the *Information Security Technology-Technical Requirement of Security Design for Classified Protection of Cybersecurity* (GB/T 25070-2019) which replaces GB/T 25070-2010.

Meanwhile, the draft regulations and guidelines on the protection of critical information infrastructure (**CII**), data processing and security assessment of outbound data transfers have been finished and the relevant authorities are now seeking opinions, including the draft *Regulations on the Security Protection of Critical Information Infrastructure, the draft Measures for Cybersecurity Censorship*, the draft *Administrative Measures on Data Security*, the draft *Measures for Security Assessment for Cross-border Transfer of Personal Information*, the draft *Guidelines for the Security Assessment of Cross-Border Data Transfer*, and the draft *Administrative Provisions on Cybersecurity Loophole*.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The *Cybersecurity Law* includes provisions on the security protection of CII. The draft *Regulations on the Security Protection of Critical Information Infrastructure* further specify the requirements on the security protection of critical information infrastructure, including CII operators' obligations relating to the setting up, suspension of operation and occurrence of security Incidents of CII, daily security maintenance, security monitoring and assessment, local data storage and security assessment of outbound data transfers, security of network products and services procured, etc.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. The *Cybersecurity Law*, the *Regulations on the Security Protection of Computer Information System*, the *National Emergency Response Plan for Cybersecurity Incidents*, and other relevant laws and regulations have provided for network operators' legal duties when facing cybersecurity Incidents, which in general could be categorised into the following:

(1) regular preventive work: network operators must adopt regular measures to prevent cybersecurity Incidents, including adopting technical measures to prevent cybersecurity violations such as computer viruses, cyberattacks and network intrusions, adopting technical measures to monitor and record the network operation status and cybersecurity events, maintaining cyber-related logs for no less than six months, etc.;

(2) emergency measures for security Incidents: network operators must develop an emergency plan for cybersecurity Incidents in order to promptly respond to security risks, to take remedial actions immediately, to notify affected data subjects, and to report the case to the competent authorities as required; and

(3) after-action review: to keep communication with and assist the authorities in finishing their investigation and review after an Incident, such as providing a summary of the cause, nature, and influence of the security Incident and improvement measures.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Conflict of laws issues may arise, as although China's cybersecurity laws and regulations in general apply to network operators within the territory of China, any activities outside China that may threaten the cybersecurity of China could also be governed by Chinese laws.

For example, in terms of import/export controls of encryption software and hardware, pursuant to the *Regulation on the Administration of Commercial Cipher Codes of China*, import of encryption products and equipment with encryption technology or export of commercial encryption products shall be approved by the national encryption administrations. Any sale of foreign encryption products by an entity or individual is prohibited.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes.

(a) The reporting obligation will be triggered by the occurrence of an Incident threatening network security.

(b) Pursuant to the *Cybersecurity Law* and relevant regulations, network operators shall at least timely notify the local government, industry regulators, public security authorities and local cyberspace administrations. Pursuant to the *Regulations of the People's Republic of China on the Security Protection of Computer Information System*, any case arising from computer information systems shall be reported to the public security authority within 24 hours. Moreover, if there is a possibility of information leakage related to national security, the national security authorities shall also be informed.

(c) At least the following contents are required to be reported: information of the notification party; description of the network security Incident; detailed information about the Incident; nature of the Incident; affected properties (if any); personal information being affected/breached (if any); preliminary containment measures that have been taken; and preliminary assessment on the severity of the Incident.

(d) If the publication of Incident-related information will jeopardise national security or public interest, then such publication shall be prohibited.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Pursuant to the *Cybersecurity Law*, the authorities support the cooperation among network operators in the collection, analysis and notification of cybersecurity information and the emergency response, in order to improve their capability for cybersecurity protection. But the releasing of cybersecurity information to the public, such as system bugs, computer viruses, network attacks and intrusions, shall be carried out in compliance with the applicable regulations.

In China, users, suppliers and research institutions are encouraged to report any potential system vulnerabilities identified to the China National Vulnerability Database, an official database operated by the National Network Emergency Response Coordination Center of China, so as to gather, verify and warn against any security vulnerabilities and to establish an effective and coordinated emergency response mechanism among all operators.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes.

(a) Under the *Cybersecurity Law*, in case of disclosure, damage or loss, or possible disclosure, damage or loss, of user information, the network operator is obligated to take immediate remedies and notify the affected users promptly. In addition, for any risk, such as a security defect or bug that is found in a network product or service, the product/service provider concerned shall inform the users of the said risk.

(b) Currently, relevant laws and regulations do not provide specific requirements about the nature and scope of information to be reported; according to the *Information Security Techniques – Personal Information Security Specification*, recommended standards formulated by the National Standardization Committee, operators shall at least inform data subjects of the general description of the Incident and its impact, any remedial measures taken or to be taken, suggestions for individual data subjects to mitigate risks, contact information of the person responsible for dealing with the Incident, etc.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

When reporting an Incident to the regulatory authorities, network operators are required to provide any information relating to the Incident as required by the authorities, even if such information involves sensitive business information or personal identifiable information, so as to effectively cooperate with the authorities in investigating and dealing with the Incident.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Any regulators identified under question 2.5 above to which network operators are required to report an Incident shall have the authority to enforce the requirements identified under questions 2.3 to 2.7. Specifically, the enforcement authorities include the Cyberspace Administration of China (the **CAC**), the Ministry of Industry and Information Technology (the **MIIT**), the Ministry of Public Security (the **MPS**), the State Secrecy Bureau, the State Encryption Administration and industry regulators, etc.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Pursuant to the *Cybersecurity Law*, in case of non-compliance, network operators may be given a warning, ordered to take rectification measures, and/or imposed fines by the relevant authorities. In case of refusal to make rectifications or of severe circumstance, further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of a business licence may be imposed by competent authorities.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

One of the first enforcement actions taken since the implementation of the *Cybersecurity Law* relates to the failure to maintain web logs. The cybersecurity team of the public security bureau of Chongqing

Municipality gave warnings to a company providing a data centre service for failure to keep a web log, as required by the *Cybersecurity Law*, and ordered it to rectify the non-compliance.

In January 2018, a local library was fined by the local public security bureau in Henan Province due to its failure to adopt technical measures to prevent computer viruses which resulted in attacks on the website. The library was imposed a fine of RMB 20,000.

Each year, the CAC, MIIT, MPS together with the National Work Group for "Combating Pornography and Illegal Publications" will initiate a special campaign called "Jingwang" (clean the internet), aiming at investigating and preventing illegal activities in cyberspace or cybercrimes. The Jingwang 2019 campaign was initiated in March 2019 and the public security authorities have successfully detected a high number of cybercrimes, including using malware to invade a third party website.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The use of Beacons may result in the collection and use of users' personal information. Pursuant to the *Cybersecurity Law*, the organisations shall notify the users and obtain their consent before collecting information. Considering the difficulty to obtain consent when collecting information through Beacons, it is generally regarded as not complying with the basic requirement under the *Cybersecurity Law*.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Relevant laws and regulations do not explicitly prohibit organisations of using Honeypots to detect and deflect Incidents in their own network.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Relevant laws and regulations do not explicitly prohibit organisations of using Sinkholes to detect and deflect Incidents in their own network.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Although industries or sectors such as telecoms, credit reporting, banking and finance, and insurance have some specific requirements with respect to the collection and protection of information, the prevention of information leakage, and the emergency response to Incidents, these requirements are, in general, in line with those under the *Cybersecurity Law* without deviations.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes. For example, the *Provisional Rules on Management of the Individual Credit Information Database* is promulgated by the People's Bank of China to ensure the secure and legitimate use of personal credit information, the *Measures of the People's Bank of China for the Protection of Financial Consumers' Rights and Interests* obliges financial institutions to ensure the security of personal financial information and the Anti-Money Laundering Law as well as the *Administrative Measures for the Identification of Clients and the Keeping of Clients' Identity Information and Transaction Records by Financial Institutions* require financial institutions to take technical measures to prevent the loss, destruction or leakage of their client's identity information or transaction data. In addition, pursuant to the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, telecommunication business operators or internet information service providers shall record information such as the staff members who perform operations on the personal information of users, the time and place of such operations, and the matters involved, to prevent user information from being divulged, damaged, tampered with or lost.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Under the *Cybersecurity Law*, if a company, as a network operator, fails to fulfil the obligation of security protection to ensure that the network is free from interference, disruption or unauthorised access, and to prevent network data from being disclosed, stolen or tampered with, fails to satisfy the mandatory requirements set forth in the applicable national standards, or fails to develop an emergency plan for cybersecurity Incidents, a warning shall be imposed on the company, and a fine will be imposed on both the company and the responsible person directly in charge if such company refuses to make rectifications or causes threats on cybersecurity.

Moreover, as mentioned in question 1.1 above, pursuant to Article 286(1) of the *Criminal Law*, if a network service provider fails to perform its duties of security protection on the information network as required by laws and administrative regulations, and refuses to correct their conduct after the regulatory authorities order them to rectify the non-performance, the network operator shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences may be sentenced.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the *Cybersecurity Law*, all network operators are required to designate a person in charge of cybersecurity, such as a CISO, to establish an emergency plan for cybersecurity Incidents, and to take technical measures to monitor and record network operation and cybersecurity events.

In addition, pursuant to Article 38 of the *Cybersecurity Law*, CII operators are required to conduct, by themselves or entrusting a service provider, an examination and assessment of their cybersecurity and the potential risks at least once a year, and submit the examination and assessment results, as well as improvement measures, to the competent authorities in charge of the security of the CII. That is to say, periodic cyber risk assessments and vulnerability assessments are mandatory for CII operators.

There is no clear requirement to include third-party vendors in the scope of the risk assessment. However, critical network equipment and special-purpose cybersecurity products provided by third-party vendors should satisfy the compulsory requirements set forth in the national standards and shall not be sold or supplied until such equipment or product successfully passes security certification or security tests by a qualified organisation.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Please refer to the answers to questions 2.5, 2.6 and 2.7 above.

In addition, listed companies may have the duty to disclose cybersecurity risks or Incidents to the China Securities Regulatory Commission or disclose such information in their annual reports, depending on whether such information is deemed as significant and required to be disclosed.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

In general, network operators' obligations in relation to cybersecurity under relevant laws and regulations include maintaining the security of the network operation, and protecting the security of network information. The *Cybersecurity Law* has established the relevant mechanism for the above purpose, such as regulations in relation to graded protection for cybersecurity, personal information protection, CII protection, cross-border data transmission, emergency response for Incidents, and security review of network products and services. Under each of these mechanisms, network operators are subject to specific obligations.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

From the perspective of individuals, if an Incident results in unauthorised access to or disclosure of personal information collected and kept by the network operator, the individuals affected could bring a lawsuit against such network operator for breach of security protection obligations or for disclosing personal information by negligence on the basis of tort pursuant to the *General Provisions of the Civil Law of the People's Republic of China* and the *Tort Law of the People's Republic of China*.

Further, as confirmed by the decision on the Sina/Maimai case by the Beijing Intellectual Property Court, user data/information is an important operating resource and confers competitive advantages to network operators. If a network operator "steals" data from its competitor by accessing the data of such competitor without authorisation, the aggrieved party could sue the infringing party for unfair competition on the basis of the *Anti-unfair Competition Law of the People's Republic of China*.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Qunar, a major online ticket-booking platform in China, and China Eastern Airlines were sued by one of its users for tort before the First Intermediate People's Court of Beijing in March 2017, as the user's personal information, including name and telephone number, was disclosed by Qunar and China Eastern Airlines to a third party who sent phishing messages to such user, claiming that the flight booked was cancelled. The court ordered Qunar and China Eastern Airlines to apologise to the plaintiff.

As mentioned in question 5.1 above, in the Sina/Maimai case, Maimai illegally accessed and collected user information from Sina without authorisation. Sina brought a lawsuit against Maimai for unfair competition, and the court upheld the claims made by Sina and ordered Maimai to stop its illegal activities, apologise in public, and compensate Sina.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Please refer to the answer to question 5.1.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations may take out insurance against Incidents, provided that such insurance categories are within the permitted scope of insurance regulations and have been approved by or filed with the China Insurance Regulatory Commission (**CIRC**). Currently, in China, there are already several insurance agents providing insurance related to Incidents such as data leakage, hacking, etc.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

So far, we are not aware of any regulation that sets out limitations specifically on insurance against Incidents. Normally, the coverage of loss will be decided through private negotiation between the insurer and the applicant, as long as such coverage does not violate mandatory regulations in China.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Article 21 of the *Cybersecurity Law* has set out several general obligations for network operators in terms of the issue of employees, including formulating internal security management systems and operation instructions, and determining a person in

charge of cybersecurity so that his responsibility will be clearly defined.

Apart from that, pursuant to Article 34 of the *Cybersecurity Law*, CII operators shall establish a dedicated security management body, designate a person in charge, and review the security backgrounds of the said person and those in key positions. Furthermore, CII operators are also obliged to provide the relevant employees with regular cybersecurity education, technical training and skill assessment.

It is understood that specific requirements on the monitoring of employees or reporting by employees may be stipulated in the internal rules or policies of network operators for the purpose of security protection.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

From the perspective of commercial practice, as companies impose confidentiality obligations on their employees (say, in the employment contract or separate confidentiality agreement or internal company rules and policies), an employee's reporting of the vulnerability of his company's network system to a third party would probably lead to a failure to fulfil such obligations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In accordance with the *Cybersecurity Law* and other relevant regulations, generally there are several enforcement agencies that are entitled to have investigatory power regarding an Incident, such as:

(1) the CAC, which is responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration; and

(2) the authority in charge of telecommunication, the public security authority and other relevant authorities of the State Council, which will take charge of protecting, supervising and administrating cybersecurity pursuant to the present regulations in China.

The specific investigatory power of the above enforcement agencies can be found in a number of laws and regulations. For example, as stated in Article 54 of the *Cybersecurity Law*, the relevant departments of the government at provincial level and above are entitled to take the following measures in case of an increasing risk of an Incident:

(1) require authorities, organs and personnel concerned to promptly collect and report necessary information;

(2) organise authorities, organs and professionals concerned to analyse and evaluate cybersecurity risks; and

(3) give warnings to the public about the cybersecurity risks and release prevention and mitigation measures.

Pursuant to Article 19 of the *Anti-Terrorism Law of the People's Republic of China* ("**Anti-Terrorism Law**"), where a risk of terrorism may arise in an Incident, the CAC, competent telecommunications department, public security department, as well as the national security department shall engage the following actions in accordance with their respective duties:

(1) order the relevant entities to stop transmission and delete the information involving terrorism and extremism; and

(2) shut down the relevant sites and cease the related services.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

First, the *Cybersecurity Law* has made it clear that network operators shall provide technical support for the public security department and the national security department specifically on two matters: 1) safeguarding national security; and 2) investigation of crimes. Second, the *Anti-Terrorism Law* explicitly states that telecommunications operators and internet service providers shall facilitate the relevant departments in terrorism cases, such as providing technical interfaces and decryption services. Moreover, for entities and individuals which engage in international network connections, public security departments may also ask them to provide information, materials and digital files on security protection matters when investigating crimes committed through computer networks connected with international networks. In several business sectors, such as the financial sector, there are also applicable laws or regulations requiring entities to coordinate with relevant industrial regulators in their investigatory activities. For example, the Anti-Money Laundering Law requires financial institutions to promptly report large amount transactions and suspicious transactions to the anti-money laundering information centre.

Susan Ning is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her publications include *New Trends of the US Personal Data Protection – Key Points of the New FCC Rules, Big Data: Success Comes Down to Solid Compliance, Does Your Data Need a "VISA" to Travel Abroad?*, and *A Brief Analysis on the Impact of Data on Competition in the Big Data Era*, among others. Susan is recognised as a "Tier 1 Lawyer" for Cybersecurity and Data Compliance in *2019 LEGALBAND China*.

Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payment, consumer goods, finance, Internet of Vehicles in dealing with network security and data compliance issues.

King & Wood Mallesons
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P. R. China

Tel: +86 10 5878 5010
Fax: +86 10 5878 5599
Email: susan.ning@cn.kwm.com
URL: www.kwm.com

Han Wu practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to multinational companies' branches in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the United States and other cross-jurisdictions. Han was elected as one of "40-under-40 Data Lawyers" by *Global Data Review* in 2018.

In the area of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity Incidents, among others.

King & Wood Mallesons
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P. R. China

Tel: +86 10 5878 5749
Fax: +86 10 5878 5599
Email: wuhan@cn.kwm.com
URL: www.kwm.com

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. Around the world, the firm has over 2,000 lawyers with an extensive global network of 27 international offices spanning Singapore, Japan, the US, Australia, the UK, Germany, Spain, Italy and other key cities in Europe as well as presences in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies and business and legal media, including *Acritas*, *Financial Times*, *ALB*, *Who's Who Legal*, *Chambers Asia-Pacific* Awards, *Euromoney*, *LEGALBAND*, *Legal Business*, *The Lawyer*, etc.

www.kwm.com

KING&WOOD MALLESONS
金杜律师事务所

Denmark

Niels Dahl-Nielsen

Daniel Kiil

Synch Advokatpartnerselskab

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking, in the narrow sense of gaining unauthorised access to another's information or to programs intended to be used in an information system, is a criminal offence punishable by a fine or imprisonment of up to one year and six months according to the Danish Criminal Code ("DCC"). In the presence of aggravating circumstances, or if the offence is of a more systematic or organised character, the punishment is imprisonment of up to six years.

In one case, a person received a penalty equal to a fine of DKK 2,000 for gaining unauthorised access to another person's social media account. In another case, a person received a two-year jail sentence for hacking his previous employer on three occasions and, among other things, deleting vital data, resulting in the company having to shut down business and spending several weeks restoring its IT systems.

Denial-of-service attacks
Denial-of-service attacks are punishable by a fine or imprisonment of up to one year according to the DCC, which criminalises preventing another from using or having access to, including the use of, its information systems.

In the presence of aggravating circumstances, or if the offence is of a more systematic or organised character, the punishment is imprisonment of up to two years.

Phishing
Phishing is, as identity theft, not criminalised as such, but usually forms part of another criminal offence such as data fraud.

In some circumstances, sending an email with false information may be punishable as falsification of documents according to the DCC. In that case, the punishment is a fine, imprisonment of up to two years or, in the presence of aggravating circumstances or in case of a high number of offences, imprisonment of up to six years according to the DCC.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Destructive attacks on IT systems are considered vandalism according to the DCC and are punishable by a fine or imprisonment of up to one year and six months. In case of repeat offenders or vandalism of a more systematic or organised character, the punishment is imprisonment of up to six years.

Destructive attacks on systems that are vital to society are punishable by a fine or imprisonment of up to six years according to the DCC.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The development or possession of malicious software is not criminalised in general. However, when accompanied with preparatory acts such as the establishment of communication channels where the source is not identifiable, the potential perpetrator may be punished for an attempt to spread the malware, which is punishable in the same manner as if the malware was spread successfully.

Manufacturing, acquisition, etc. of information that can be used to identify means of payment or generated payment card numbers is punishable by a fine or imprisonment of up to one year and six months according to the DCC. In the presence of aggravating circumstances, the punishment is imprisonment of up to six years.

According to the DCC, unauthorised acquisition or communication of access codes, or other means of access to information systems reserved for paying users, is a criminal offence and punishable by a fine or imprisonment of up to one year and six months. In the presence of aggravating circumstances, the punishment is imprisonment of up to six years.

Possession for commercial purposes, sale, etc., of tools intended to bypass DRM protection is a criminal offence and punishable by a fine according to the Danish Copyright Act.

Possession, manufacturing, etc., of and advertising for decoders or other decoding equipment for the purpose of giving unauthorised access to the contents of an encrypted radio or TV programme is punishable with a fine according to the Danish Radio and Television Act. Intentional offences in the presence of aggravating circumstances are punishable by imprisonment of up to one year and six months.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft is not criminalised as such but usually leads to or forms part of another criminal offence such as falsification of documents, hacking, theft, fraud, or data fraud. In one case, a person received a jail sentence of two years and six months for installing keyloggers on public library computers to copy the electronic ID usernames and passwords of library visitors and subsequently using the information to commit data fraud.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The Danish Act on Trade Secrets criminalises unlawful acquisition, use, and disclosure of trade secrets and, *inter alia*, eases the

requirements for the use of provisional and precautionary measures. A trade secret is defined as information that is not generally known, has commercial value because it is a secret, and has been subject to reasonable measures to keep it secret.

Employees of telecommunications companies are subject to specific legislation regarding information about the usage of the company's service under the Danish Telecommunications Act.

Data fraud is punishable by imprisonment of up to one year and six months, or up to eight years if the offence is of a particularly aggravated nature according to the DCC. Data fraud includes, in particular, unauthorised wire transfers and the use of false or stolen credit card details. In one case, a financial adviser received a jail sentence of one year and six months for illegally transferring around DKK 1.2 million from around 60 customer accounts to his own or other accounts over a period of more than seven years.

Unauthorised reproduction or making available to the public of copyright protected works is punishable by a fine, or imprisonment of up to one year and six months if the offence is committed intentionally and in the presence of aggravating circumstances according to the Danish Copyright Act. Intellectual property infringements of a particularly aggravated nature are punishable by imprisonment of up to six years according to the DCC.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Interception of email and other electronic messages by cutting it off from the intended recipient or familiarising one with its contents is punishable by a fine, imprisonment of up to one year and six months, or imprisonment of up to six years in the presence of aggravating circumstances according to the DCC.

Opening an email that has been wrongly addressed to someone is not criminalised. However, forwarding such a message may, depending on its contents, be punishable as unauthorised communication of messages concerning another's private matters according to the DCC.

Commercial sale or a greater dissemination of codes or other means of access to an information system not available to the public is punishable by a fine or imprisonment of up to one year and six months according to the DCC. In the presence of aggravating circumstances, the punishment is imprisonment of up to six years according to the DCC.

According to the DCC, unjustified use of information resulting from another person's hacking, interception of messages, or sale or dissemination of codes or other means of access to an information system not available to the public is punishable in the same manner as the original offence.

Failure by an organisation to implement cybersecurity measures

Under the GDPR, a data controller's or processor's failure to implement appropriate security measures is subject to an administrative fine.

The failure of the board of directors of a limited liability company to ensure an adequate level of security for the company is punishable by a fine and may result in civil liability as further described under question 4.1.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The DCC applies to criminal offences committed on foreign territory when the offence is committed by a Dane or a person living in Denmark and the act is also criminalised in the foreign country (double criminality).

In relation to offences that depend on or are influenced by an intended or occurred consequence of the offence, the offence is considered as having occurred where the perpetrator intended for the consequence to materialise. As such, the Danish criminal jurisdiction covers offences where the perpetrator was not on Danish territory when committing the criminal offence if his actions had or were intended to have a consequence on Danish territory, as is often the case concerning cybercrime.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The DCC states certain general circumstances that shall be considered when determining criminal sanctions, e.g., whether the perpetrator has denounced himself and pled guilty to the offence. Further, subject to a specific assessment of the circumstances, there is a general possibility of remission or discharge.

Under the GDPR, when deciding whether to impose an administrative fine and deciding on the amount of the fine, there are several mitigating factors to be considered, such as how the supervisory authority became aware of the infringement and the degree of cooperation with the supervisory authority in order to remedy the infringement.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The duty of confidentiality of persons operating within the public administration, according to the Danish Public Administration Act, as well as lawyers, doctors, and pastors, entails an obligation to implement adequate security measures to protect confidential information.

Destructive attacks of considerable proportions on IT systems and destructive attacks on systems that are vital to society are punishable as terrorism according to the DCC, when the act can cause serious damage to a country or an international organisation and the offence is committed in a manner that may threaten human life or cause considerable economic losses. Further, the perpetrator must have committed the offence with the intention of seriously intimidating a population, forcing the hand of public authorities or an international organisation, or destabilising or destroying the fundamental structures of a country or an international organisation. The punishment is imprisonment up to a life sentence.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Danish law does not provide a consolidated approach to cybersecurity. The following acts and orders relate directly or indirectly to cybersecurity.

Company law
- The Danish Companies Act.

Criminal law
- The Danish Criminal Code.

Critical infrastructure
- The Danish Act on Network and Information Security of Domain Name Systems and Certain Digital Services.
- The Danish Act on Requirements of Security of Network and Information Systems within the Health Sector.
- The Danish Act on Security of Network and Information Systems for Operators of Essential Internet Exchange Points etc.
- The Danish Act on Security of Network and Information Systems in the Transport Sector.

Data protection
- The General Data Protection Regulation (the GDPR).
- The Danish Data Protection Act.

Health sector
- The Danish Order on Health Preparedness Planning.
- The Danish Order on Health Records.

Intellectual property
- The Danish Copyright Act.

Financial services sector
- The Danish Financial Business Act.
- The Danish Act on Payment Services.
- The Danish Order on Management and Control of Banks etc.
- The Danish Order on Outsourcing.

Telecommunications sector
- The Danish Radio and Television Act.
- The Danish Telecommunications Act.

Other sector-specific requirements to emergency preparedness and response
- The Danish Order on Preparedness for the Natural Gas Sector.
- The Danish Order on Preparedness for the Electricity Sector.
- The Danish Order on Preparedness Relating to Offshore Oil and Gas Operations.
- The Danish Order on Preparedness Relating to Marine Pollution from Oil and Gas Installations etc.
- The Danish Order on Railway Undertakings and Railway Infrastructure Managers.
- The Danish Order on Risk-Based Municipal Emergency Services.

Other
- The Constitutional Act of the Kingdom of Denmark.
- The Danish Act on Television Surveillance.
- The Danish Act on the Centre for Cyber Security.
- The Danish Act on Trade Secrets.
- The EU Cybersecurity Act.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Network and Information Systems Directive is implemented into Danish law with several sector-specific acts (listed under question 2.1 under critical infrastructure). The implementing legislation does not exceed the requirements of the directive.

Operators of essential services are, according to the relevant sector-specific legislation, required to implement an appropriate security level to control the risk to security in the network and information systems used for their activities. An operator of an essential service is generally defined as i) a unit that delivers a service that is essential for the maintenance of critical societal functions, ii) where the delivery of the service depends on networks and information systems, and iii) an Incident would have a highly disruptive effect on the delivery of the service.

Providers of digital services are subject to certain requirements according to the Danish Act on Network and Information Security of Domain Name Systems and Certain Digital Services. Digital services are generally online marketplaces, online search engines, and cloud computing-services that are not considered essential services. Providers of digital services are also required to implement an appropriate security level.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Certain companies are required to maintain adequate levels of cybersecurity, mainly by means of policies, as further described under questions 4.1–4.4.

Insofar as information that qualifies as personal data according to the GDPR is involved, data controllers and processors are required to implement an adequate level of security in relation to the risks that are presented by the processing. Further, where a type of processing is likely to result in a high risk to individuals, the data controller shall carry out an assessment of the impact of the envisaged processing operations.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Currently, no issues regarding conflict of laws have been identified, although different Acts may regulate similar areas.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

According to the GDPR, the data controller shall notify the supervisory authority of a personal data breach without undue delay after becoming aware of it. A data processor shall notify the data controller of a breach without undue delay.

Operators of essential services are required to report Incidents with an impact on the continuity of the services they deliver. The recipient of the report depends on the sector of the operator. For instance, according to the Danish Act on Net and Information Security for Domain Name Systems and Certain Digital Services, Incidents must be reported to the Danish Business Authority and the Danish Centre for Cyber Security. Such a report must namely contain information as to the number of affected users, the duration of the Incident, and the geographical spread in relation to the area affected by the Incident. The relevant regulator can publish information about specific Incidents when necessary to prevent or manage an Incident in progress.

Similarly, providers of digital services are required to report Incidents with a substantial impact on the services they deliver to the Danish Business Authority and the Danish Centre for Cyber Security.

Providers of financial services are required to report certain Incidents to the relevant authorities, primarily the Financial Supervisory Authority, the Danish Business Authority and the Danish Centre for Cyber Security.

The Danish Business Authority has oversight of the main sections of the Danish Telecommunication Act but, depending on the type of Incident, other authorities may be involved, especially the Danish Centre for Cyber Security.

The Danish Act on Payment Services puts obligations on providers of payment services to report Incidents to the authorities and to the users of the payment services if there is a risk that their transactions may be affected. The report to the authorities must, among other things, describe the reason for the Incident and, if applicable, the attack methodology.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Restrictions in relation to general rules on, e.g., confidentiality and personal data protection may limit the ability of organisations to share information related to Incidents or potential Incidents.

Companies can voluntarily share information related to Incidents with the Danish Centre for Cyber Security. Such voluntary notifications are exempt from the rules regarding public access to documents and allow the Danish Centre for Cyber Security to assist authorities and companies in case of an Incident.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

According to the GDPR, data controllers are required to notify data subjects without undue delay of personal data breaches that are likely to result in a high degree of risk to the rights and freedoms of the data subjects.

The Danish Act on Payment Services puts obligations on providers of payment services to report Incidents to the users of the payment services if there is a risk that their transactions may be affected.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, but insofar as the Incident relates to information that qualifies as personal data under the GDPR, the requirements of the GDPR must be respected when processing the data.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Danish Data Protection Agency is responsible for enforcing the requirements under the GDPR.

The regulator responsible for enforcing the requirements for operators of essential and digital services depends on the sector of the operator in question.

The Danish Business Authority has oversight of the main sections of the Danish Telecommunication Act.

The regulators responsible for enforcing the requirements under the Danish Act on Payment Services and for providers of financial services depends on the nature of the breach, but are primarily the Financial Supervisory Authority, the Danish Business Authority and the Danish Centre for Cyber Security.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Failure to comply with the requirements under the GDPR is subject to an administrative fine.

The failure of an essential service to comply with the requirements for such a service is punishable by a fine.

The failure to comply with the requirements under the Danish Telecommunications Act is punishable by a fine.

The failure to comply with the requirements under the Danish Act on Payment Services is punishable by a fine.

The failure to comply with requirements related to providers of financial services is subject to a fine and may be subject to imprisonment.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There have been no notable examples of enforcement in relation to non-compliance with regulatory cybersecurity requirements thus far.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Yes. However, relevant data protection and ePrivacy legislation must be assessed if any personal data is processed, e.g. an IP-address. If this is the case, the data subject must be informed of the legal grounds that are used for the processing of personal data.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Yes. Further, as per 1 July 2019, the Danish Centre for Cyber Security is permitted to use honeypots to gather information on the attack methods and tools used by cyber threat actors. Such honeypots can, where appropriate and in agreement with the relevant organisation, be used on the networks and equipment of the authorities and companies that are connected to the Danish Centre for Cyber Security's network security service.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Yes. Further, as per 1 July 2019, the Danish Centre for Cyber Security is permitted to use sinkholes to prevent, stop or limit an imminent or ongoing Incident.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, the market practice varies across business sectors due to extensive sector-specific regulation. However, there are no common deviations from any strict legal requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes, companies within the financial services sector are, *inter alia*, required to adopt a cybersecurity policy, prepare a contingency plan, and comply with an extensive set of requirements when outsourcing key activity areas.

Regarding the telecommunications sector, providers of public electronic communications networks or services are primarily subject to legal requirements under the Danish Telecommunications Act. Such providers are, *inter alia*, obliged to register themselves with the police and comply with certain rules regarding equipment, information security and emergency situations.

It should also be noted that a new EU directive (the EECC) which establishes new telecom rules in the EU was formally adopted on 20 December 2018. Denmark has yet to implement the directive which must be implemented in domestic law by the Member States before 21 December 2020.

Further, as described under question 2.5, providers of essential services and digital services are required to report Incidents as per the above.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

According to the Danish Companies Act, in limited liability companies that have a board of directors, the board must ensure that adequate risk management and internal control procedures are established. This entails an obligation to maintain an overview of cybersecurity risks and to ensure an adequate level of cybersecurity. If such measures are found to be inadequate, an Incident may amount to a breach of the directors' duties.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Certain companies, especially in the financial sector and ones responsible for critical infrastructure (NIS Directive), are required to maintain security policies, especially related to IT security. Further, the GDPR requires technical and organisational measures to be in place.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

As per the above, certain companies are required to maintain security policies. Under certain circumstances, such policies, etc., must be disclosed to the relevant authorities.

Further, the obligations of the board of directors may include an obligation to take cybersecurity risks into account in the company's annual report.

Additionally, listed companies may be required to disclose information (regardless of whether it derives from a cybersecurity breach or not) that may affect the price of the company shares.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, besides sector-specific requirements, companies are not subject to any other specific requirements in relation to cybersecurity.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

A person or an organisation that has suffered damages as a result of another organisation's action or omission, namely by failing to comply with regulatory requirements, can claim compensation for the damages suffered. The injured party will normally have to prove that he has suffered damages, that there is a basis of liability, and that there is a causal link between the damages suffered and the action or omission giving rise to his claim.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There have been no notable civil cases in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes, there is a potential liability in tort in relation to an Incident, but this would normally be subsidiary to other damages in Danish law.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, cyber risk insurances are permitted and gaining in popularity.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No. However, it is unclear whether it is possible to insure yourself against regulatory fines or not.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The rights of employers to monitor their employees are generally regulated by labour law regulations. Such monitoring must be reasonably justified on the grounds of the operations of the employer.

There are no general requirements regarding the reporting of cyber risks, etc., by employees to their employer. Due to the duty of loyalty arising from the employment contract, however, an employee may, depending on the circumstances, be considered to be obliged to report Incidents to the employer.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The Danish Act on Trade Secrets may prohibit or limit the reporting of cyber risks, etc., when such reporting involves unlawful acquisition, use, and disclosure of trade secrets. However, the act includes a general exception that allows disclosure, etc., of trade secrets when acting as a whistleblower.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The law enforcement authorities have various common powers of investigation, depending on the nature of the given case as well as which authority is investigating it.

The Danish Data Protection Agency is authorised to carry out planned and *ad hoc* investigations of authorities, companies and other data controllers and data processors. In connection with such investigations, the Danish Data Protection Agency can, *inter alia*, order any information it requires for the performance of its tasks to be provided, and obtain access to any premises of the data controller or processor.

The Centre for Cyber Security can, *inter alia*, in a number of circumstances, process package and traffic data from networks of affiliated authorities and organisations without a court order.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Providers of certain electronic communications services are obligated to make it possible for law enforcement authorities to gain insight into or listen in on communications.

Acknowledgment

We would like to thank junior lawyer Kristoffer Rosenquist Kirk for his valuable contribution to this chapter.

Niels Dahl-Nielsen is a co-founder of Synch in Copenhagen. Niels heads Synch's practice within data protection and cybersecurity and has a great deal of experience within those same areas. Niels Dahl-Nielsen mainly represents companies in the IT industry within various segments – in particular software development and software consultancy companies in all matters related to data protection and cybersecurity. Furthermore, Niels has been a speaker at various conferences on privacy and cybersecurity, including NATO's 2nd Cyber Security Conference at a maritime training centre in Crete, Greece.
Niels Dahl-Nielsen is a member of the Danish Data Protection Association.

Synch Advokatpartnerselskab
Strandvejen 58
1. Sal, 2900 Hellerup
Denmark

Tel: +45 7027 8899
Fax: +45 7027 8898
Email: niels.dahl-nielsen@synchlaw.dk
URL: www.synchlaw.se/da

Daniel Kiil joined Synch in 2018 and works as a lawyer. He is specialised within IT, technology and personal data protection. Further, he has experience within corporate and intellectual property law. Daniel works with Synch's team in Scandinavia. He previously worked at Rambøll Management Consulting as a Senior Legal Consultant. Previously, he worked as a lawyer at DXC Technology.

Synch Advokatpartnerselskab
Strandvejen 58
1. Sal, 2900 Hellerup
Denmark

Tel: +45 7027 8899
Fax: +45 7027 8898
Email: daniel.kiil@synchlaw.dk
URL: www.synchlaw.se/da

Synch Advokatpartnerselskab is a business-oriented law firm with innovation and technology at its heart. We believe that lawyers and legal services always need to be in synch with the business environment. Legal services are to be provided in a pragmatic and accessible way. This is equally true for large, established industry companies as it is for small, fast-growing start-ups.
Synch wants to simplify the management of legal matters, both by providing packaged solutions and by making the best use of technology. In this way, Synch is able, and desires, to work more closely with its customers than traditional law firms, almost like an insourced legal department, taking part in the customers' daily business. Several of our lawyers are highly regarded individuals within their area of specialty and this has been recognised by the leading ranking institutes of legal services. Today Synch has offices in Copenhagen, Oslo, Silicon Valley and Stockholm.

www.synchlaw.se/da

England & Wales

Nigel Parker

Alexandra Rendell

Allen & Overy LLP

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes. Under the Computer Misuse Act 1990, it is an offence to cause a computer to perform any function with the intent to secure unauthorised access to any program or data held in a computer (or enable such access to be secured). On indictment, the maximum penalty is two years' imprisonment or an unlimited fine, or both. In 2012, two separate cases were prosecuted involving unauthorised access to Facebook accounts and Facebook's computers (respectively). In the first instance, the individual was sentenced to four and eight months concurrent in a young offender institution. In the latter, the individual was sentenced to four months' imprisonment.

Denial-of-service attacks
Yes. Under the Computer Misuse Act 1990, it is an offence to do any unauthorised act in relation to a computer that a person knows to be unauthorised, with the intent of impairing the operation of any computer, preventing or hindering access to any program or the data held in any computer, impairing the operation of any program or the reliability of any data, or enabling any of the above. On indictment, the maximum penalty is 10 years' imprisonment or an unlimited fine, or both. In 2013, an individual was sentenced to two years' imprisonment in relation to denial-of-service attacks against various websites and targeting two private individuals.

Phishing
Yes. See the answer in respect of hacking.

Under the Fraud Act 2006, phishing could also constitute fraud by false representation if (for example) an email was sent falsely representing that it was sent by a legitimate firm. On indictment, the maximum penalty is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes. See the answer in respect of denial-of-service attacks.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Yes. Under the Computer Misuse Act 1990, it is an offence to make, adapt, supply or offer to supply any article intending it to be used to commit, or which may be likely to be used to commit, an offence under section 1 (see the answer in respect of hacking) or section 3 (see the answer in respect of denial-of-service attacks) of the Act. On indictment, the maximum penalty is two years' imprisonment or an unlimited fine, or both.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes. Under the Fraud Act 2006, it is an offence to dishonestly make a false representation, knowing that the representation was or may be untrue or misleading, with the intent of making a gain for yourself or another or causing a loss or risk of loss to another (i.e. fraud by false representation). On indictment, the maximum penalty is 10 years' imprisonment. In 2014, an individual was convicted of offences under the Fraud Act 2006 and Computer Misuse Act 1990 (in relation to stolen bank and credit card details) and was sentenced to a total of three years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Yes. This may constitute an offence under the Computer Misuse Act 1990 (such as hacking) as well as a financial crime, such as theft (under the Theft Act 1990). A breach of confidence or misuse of private information is actionable as a common law tort, but not as a criminal offence in itself.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Please see above.

Failure by an organisation to implement cybersecurity measures
Under the Data Protection Act 2018 (and the EU General Data Protection Regulation), organisations are required to implement technical and organisational measures to safeguard personal data, which may involve implementing cybersecurity measures. A failure to implement these measures is not, in itself, a criminal offence. However, the Information Commissioner's Office (**ICO**) may investigate such a failure (if, for example, an Incident occurred and this triggered an investigation) and issue an enforcement notice requiring the organisation to comply with its obligation to implement appropriate security measures. Failure to comply with such an enforcement notice is a criminal offence. The UK has adopted a similar approach in respect of enforcement of obligations to implement security measures under the Network and Information Systems Regulations 2018.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes. For certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks), the offence will be committed where there is a "significant link to the domestic jurisdiction". This includes the person committing the offence being in the UK, the target computer being in the UK or a UK national committing the offence while outside the UK (provided in the latter instance that the act was still an offence in the country where it took place).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There is an exemption for certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks) in respect of an enforcement officer acting in accordance with legislation to facilitate inspection, search or seizure without a person's consent. There are no general defences under the Computer Misuse Act 1990.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Certain terrorism offences may arise in relation to cybersecurity. For example, under the Terrorism Act 2000, it is an offence to take any action designed to seriously interfere with or seriously disrupt an electronic system if this is designed to influence the government or intimidate the public or a section of the public, or for the purpose of advancing a political, religious, racial or ideological cause. In this context, offences under UK terrorism legislation also include planning, assisting or collecting information on how to commit an act of terrorism. There have been a number of prosecutions of terrorism offences that involved seizure of the suspect's computer to secure evidence of the offence.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The UK legal framework for cybersecurity is dispersed with a number of different laws that may apply depending on the context of the Incident and the nature of the organisation involved.

- To the extent that Incidents involve personal data, the Data Protection Act 2018 will apply alongside the EU General Data Protection Regulation (**GDPR**). The Data Protection Act 2018 specifies provisions applicable to the UK, as permitted by the GDPR, as well as setting out data protection requirements for national security and other areas of law outside EU law, such as immigration.
- In respect of telecommunications, public electronic communications network providers and public electronic communications service providers are subject to cybersecurity obligations under the Communications Act 2003.
- Public electronic communications service providers are also subject to cybersecurity obligations under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**) in respect of personal data.
- The Network and Information Systems Regulations 2018 (**NIS Regulations**) implemented the Network and Information Systems Directive into UK law (see the answer to question 2.2).
- Public companies are subject to additional governance obligations under the Companies Act 2006, Disclosure and Transparency Rules in the Financial Conduct Authority (**FCA**) Handbook, Listing Rules in the FCA Handbook and the risk management and control provisions in the UK Corporate Governance Code, which can directly or indirectly relate to cybersecurity.
- The Regulation of Investigatory Powers Act 2000 (**RIPA**) governs the investigative powers of law enforcement, such as surveillance and interception of communications data. RIPA will ultimately be replaced by the Investigatory Powers Act 2016, the operative provisions of which are not yet all in force.
- The Computer Misuse Act 1990 sets out various cybercrime offences (see the answers to question 1.1), which may be prosecuted in conjunction with offences under the Theft Act 1968 or the Fraud Act 2006.
- The Official Secrets Act 1989 may also apply in respect of servants of the Crown or UK government contractors, and creates offences in relation to disclosure (or failure to secure) certain information which may be damaging to the UK's interests.
- Various common law doctrines may also apply in respect of civil actions (see the answer to question 5.1).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Cybersecurity requirements in the telecommunications sector are set out in the Communications Act 2003 (for example, in respect of maintaining the security and integrity of public electronic communications networks and public electronic communications services). These requirements apply to providers of public electronic communications networks and public electronic communications services, and include taking measures to prevent or minimise the impact of Incidents on end users and on interconnection of networks.

Financial services infrastructure providers may be regulated by the FCA and subject to the requirements in the Senior Management Arrangements Systems and Controls part of the FCA Handbook (see the answer to question 3.2). These organisations will be operators of essential services for the purposes of the Directive.

The NIS Regulations were published in the UK on 19 April 2018 and came into force on 10 May 2018. The NIS Regulations provide than an 'operator of essential services' must comply with certain security duties, including a duty to notify Incidents to the relevant competent authority. The NIS Regulations identify sector-based competent authorities (for sectors covering energy, transport, health, drinking water supply and distribution and digital infrastructure) with the National Cyber Security Centre (**NCSC**) as the UK's single point of contact for Incident reporting. The NCSC will also undertake the role of the Computer Security Incident Response Team.

However, the NCSC will not have a regulatory function and, in its role as the Computer Security Incident Response Team, will only respond to Incidents which arise as a result of a cyber-attack and which have been notified to it by the competent authorities. The NIS Regulations introduce a range of penalties that can be imposed by the relevant competent authority or the ICO (in the case of digital service providers). These range from £1 million for any contravention of the NIS Regulations which the relevant authority determines could not cause an Incident, up to £17 million for a material contravention of the NIS Regulations which the relevant authority determines has caused, or could cause, an Incident resulting in immediate threat to life or significant adverse impact on the United Kingdom economy. This maximum fine is broadly aligned to the maximum level of fine under the GDPR.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Data Protection Act 2018 (and the GDPR), if the organisation is a data controller in respect of personal data (i.e. it determines how and why personal data is processed) it will be required to implement appropriate technical organisational measures to ensure a level of security of that personal data appropriate to the risk, including the risk of accidental or unlawful disclosure of or access to that data.

The NIS Regulations also require operators of essential services and digital service providers to take appropriate and proportionate technical and organisational risk management measures, including to prevent and minimise the impact of Incidents.

Under PECR, a public electronic communications service provider must take appropriate technical and organisational measures to safeguard the security of their service and maintain a record of all Incidents involving a personal data breach in an inventory or log. This must contain the facts surrounding the breach, the effects of the breach and the remedial action taken by the service provider.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Yes. Obligations to implement effective security measures, systems and controls may conflict with Applicable Laws relating to unlawful interception of communications. Under RIPA, it is an offence to intentionally and without lawful authority intercept a communication in the course of its transmission. Interception will be lawful if: (a) both sender and recipient have consented; (b) the interception is carried out by a communications service provider for purposes connected with the operation of that service or to prevent fraudulent or improper use of that service; (c) the government has issued a warrant; or (d) the interception is authorised by other regulations.

In respect of the latter, an organisation may lawfully monitor communications of employees in certain circumstances under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (see the answer to question 7.1).

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Data Protection Act 2018 and the GDPR, a data controller will be required to notify an Incident involving personal data to the ICO without undue delay and, where feasible, within 72 hours after becoming aware of it unless it is unlikely to result in risks to individuals. This notification must include: (a) a description of the nature of the Incident (including, where possible, the categories and approximate number of affected individuals and the categories and approximate number of personal data records concerned); (b) the name and contact details of a contact point where the affected individual can obtain further information (which will be the organisation's data protection officer if there is one); (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, by the organisation to address the Incident and mitigate possible adverse effects. In certain circumstances, the Incident will also need to be notified to affected data subjects (see the answer to question 2.7).

Under the Data Protection Act 2018, the ICO is not permitted to publicise any information that has been disclosed to it (for example, through notification of an Incident) if that information relates to an identified or identifiable individual or business and is not already in the public domain. However, this restriction on publication will not apply in certain cases, such as if the ICO determines that publication is in the public interest. The ICO's practice is not to publicise data breach notification information unless it has taken public enforcement action in relation to the breach, or publication is necessary in the public interest (e.g. to allay public concern).

The NIS Regulations also require operators of essential services and digital service providers to report Incidents to the relevant competent authority without undue delay. The relevant authority may inform the public where public awareness is needed either to prevent or resolve the Incident, or where this would otherwise be in the public interest, but the organisation will be consulted before disclosure to the public is made to preserve confidentiality and commercial interests.

The NCSC publishes a weekly threat report on its website, with content drawn from recent open source reporting, which details cyber threat information, known network and software vulnerabilities and other information organisations and individuals may find useful. However, there is no obligation for organisations to report threat information to the NCSC to compile these reports.

Under the Communications Act 2003, a public electronic communications network provider must notify Ofcom of a breach of security that has a significant impact on the network's operation. Further, a public electronic communications service provider must notify Ofcom of a breach of security that has a significant impact on the operation of the service.

Similarly, under PECR, a public electronic communications service provider must notify the ICO of a data breach within 24 hours of becoming aware of the 'essential facts' of the breach. The notification must include: (a) the service provider's name and contact details; (b) the date and time of the breach (or an estimate); (c) the date and time the breach was detected; (d) basic information about the time of the breach; and (e) basic information about the personal data concerned.

Organisations that are regulated by the FCA are also required to notify the FCA of any significant failure in the organisation's systems and controls under Chapter 15.3 of the Supervision Manual of the FCA and PRA Handbooks, which may include Incidents that involve data loss. Similarly, under European Banking Authority guidelines on major Incident reporting under the revised Payment Services Directive, payment service providers are required to report major operational or security Incidents to the competent authority within four hours from the moment the Incident was first detected, with intermediate updates and a final report delivered within two weeks after business is deemed back to normal.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations are permitted to voluntarily share information with other regulatories or other authorities outside the UK, or with other private sector organisations or trade associations. However, if the Incident involves personal data, any such disclosures must be made in accordance with the requirements of data protection laws. For example, disclosures to regulatory or other authorities outside the UK must comply with restrictions on cross-border transfers of personal data.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the Data Protection Act 2018 and the GDPR, a data controller will be required to notify affected individuals of an Incident without undue delay if the Incident involves personal data and is likely to result in a high risk to the rights and freedoms of those individuals. This notification must include: (a) a description of the nature of the Incident; (b) the name and contact details of a contact point where the affected individual can obtain further information (which will be the organisation's data protection officer if there is one); (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, by the organisation to address the Incident and mitigate possible adverse effects.

Under PECR, a public electronic communications service provider must notify affected subscribers or users of an Incident without unnecessary delay if that Incident is likely to adversely affect their personal data or privacy. The service provider should provide a summary of the Incident, including the estimated date of the breach, the nature and content of personal data affected, the likely effect on the individual, any measures the service provider has taken to address the Incident and information as to how the individual can mitigate any possible adverse impact. No notification is required if the service provider can demonstrate to the ICO's satisfaction that the data that has been breached was encrypted or was rendered unintelligible by similar security measures.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Reporting obligations under data protection laws will only apply to the extent that the Incident involved personal data. IP addresses and email addresses may constitute or comprise personal data. Reporting obligations under the Communications Act 2003, PECR or FCA rules may apply regardless of the information that was subject to the Incident.

Listed companies may also be required to notify an Incident to the FCA if it would constitute price-sensitive information (see the answer to question 4.3).

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Under data protection laws (the Data Protection Act 2018, the GDPR and PECR), the relevant regulator is the ICO (https://ico.org.uk/).

Under the Communications Act 2003, the relevant regulator is Ofcom (https://www.ofcom.org.uk/).

Under the FCA Handbook, the relevant regulator is the FCA (https://www.fca.org.uk/).

Schedule 1 to the NIS Regulations identifies sector-based competent authorities (https://www.legislation.gov.uk/uksi/2018/506/schedule/1/made).

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Under the Data Protection Act 2018 and the GDPR, failure to report an Incident involving a personal data breach, or to implement appropriate security measures, can incur a fine of up to the higher of 2% of annual worldwide turnover or EUR10 million.

Under PECR, failure by a public electronic communications service provider to notify an Incident involving a personal data breach to the ICO can incur a £1,000 fixed fine. A failure by a public electronic communications service provider to take appropriate technical and organisational measures to safeguard the security of their service can incur a fine of up to £500,000 from the ICO.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In October 2016, the ICO issued a then-record £400,000 fine to telecoms company TalkTalk for security failings that allowed a cyber

attacker to access customer data. The ICO investigation found that the attack took advantage of a technical weakness in TalkTalk's systems which could have been prevented if TalkTalk had taken 'basic steps' to protect customer data.

In June 2017, the ICO issued a £100,000 fine to Gloucester City Council after it suffered a cyber attack that allowed the attacker to gain access to financial and sensitive personal information relating to between 30 and 40 former or current staff. In this case, the 'heartbleed' vulnerability was widely publicised in the media and the Council failed to apply an available patch for the affected software.

In July 2018, the ICO announced an intention to issue a fine of £500,000 to Facebook in relation to the ICO's investigation into data analytics and political campaigns. The fine relates to two breaches of the Data Protection Act 1998, one in relation to a failure to safeguard people's information, and a second in relation to transparency failings. This is the maximum fine permitted under the Data Protection Act 1998, which was the applicable regime in this instance.

In July 2019, in the first fine to be announced by the ICO under the GDPR, the ICO announced an intention to issue a fine of £183.39 million to British Airways following an Incident in September 2018. This Incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this Incident, which is believed to have begun in June 2018.

Also in July 2019, the day after the announcement of the British Airways fine, the ICO announced further plans to fine Marriott International £99.2 million following a data breach affecting Marriott subsidiary Starwood's guest reservation database. A variety of personal data contained in approximately 339 million guest records globally were exposed by the Incident, of which seven million related to UK residents. It is believed the relevant vulnerability began in 2014, but was not discovered until 2018. The ICO found that Marriott failed to undertake sufficient due diligence when it bought the Starwood hotels group in 2016, and should have done more to secure its systems.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are no specific laws prohibiting the use of web beacons in the UK. However, where use of a web beacon involves processing personal data, the organisation's use of the web beacon must be in accordance with the requirements of data protection laws.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no specific laws prohibiting the use of honeypots in the UK.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are no specific laws prohibiting the use of sinkholes in the UK.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Certain sectors, such as financial services and telecommunications, are more incentivised to avoid the cost and reputational impact of Incidents. In some organisations, cybersecurity practice is driven not only by compliance with Applicable Laws but also the desire to promote good 'cyber hygiene' culture. For example, although there is no legal requirement to train employees in cyber risks, many organisations do and may carry out simulations (such as phishing simulations and 'war games') as a matter of good practice.

Public sector organisations (such as the National Health Service) and government authorities are subject to additional reporting guidelines issued by the central government, in addition to disclosure obligations under Applicable Laws.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial services organisations that are regulated by the FCA are subject to the FCA Handbook, which includes Principles for Business and the Senior Management Arrangements Systems and Controls (**SYSC**). Under SYSC 3.2.6R, regulated financial services organisations are required to take reasonable care to establish and maintain effective systems and controls for compliance with regulatory requirements and standards and for countering risk that the organisation may be used to further financial crime. Further, under SYSC 3.1.1R, the organisation is required to maintain adequate policies and procedures to ensure compliance with those obligations and countering those risks. These requirements extend to cybersecurity issues. For example, the FCA has previously fined Norwich Union Life (£1.26 million) and three HSBC firms (£3 million) for failure to have adequate systems and controls in place to protect customer confidential information and manage financial crime risk.

In respect of telecommunications, public electronic communications network providers and public electronic communications service providers must take appropriate technical and organisation measures to manage risks to the security of the networks and services, including to minimise the impact of Incidents. Public electronic communications network providers must also take all appropriate steps to protect, so far as possible, the availability of that provider's network.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Directors are required, under the Companies Act 2006, to promote the success of the company for the benefit of its members as a whole and exercise reasonable skill, care and diligence in performing their role. It is up to the board of directors of each company to ensure that the board has the relevant competence and integrity to exercise these duties in view of the risk to the company as a whole,

including the risk of Incidents. A failure to prevent, mitigate, manage or respond to an Incident may be a breach of directors' duties if, for example, the failure resulted from a lack of skill, care and diligence on the part of the relevant director.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

No, there are no specific requirements in this respect. However, listed companies are required, under the UK Corporate Governance Code, to set up certain committees with responsibility for specific areas, such as audit. Financial services companies may also be required to have a risk committee. These committees may, as part of their functions, conduct risk assessments that cover cyber risk. The UK Corporate Governance Code, which was updated from 1 January 2019, emphasises the board's responsibility to determine and assess the principal risks facing the company. This responsibility extends to a robust assessment of the company's emerging risks, which would cover cyber risk.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the Disclosure and Transparency Rules set out in the FCA Handbook, listed companies are required to disclose an Incident if the Incident amounts to inside information that may affect the company's share price. For example, theft of business-critical intellectual property is likely to be price-sensitive information.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

There are a number of potential civil actions that may be brought in relation to any Incident, for example:

Breach of confidence. First, the information itself must have the necessary quality of confidence about it. Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.

Breach of contract. This could take any form from a breach of a commercial contract to an employee's terms and conditions of employment.

One example may be in relation to an International Organisation for Standardization (**ISO**) compliance standard in relation to information security and risk management. Although a failure to meet such a standard is not enforced by the ISO, if a party has contractually agreed or warranted that it complies with an ISO standard, a failure to do so will be a breach of contract.

Breach of trust. A person who owes a fiduciary duty to another may not place him or herself in a situation where s/he has a personal interest that may conflict with the interest of the person to whom the fiduciary duty is owed. If an Incident is caused by an employee or a director, a breach of trust/fiduciary duty may be claimed.

Causing loss by unlawful means. A defendant will be liable for causing loss by unlawful means where s/he intentionally causes loss to the claimant by unlawfully interfering in the freedom of a third party to deal with the claimant.

Compensation for breach of the Data Protection Act 2018 (and GDPR). Individuals who suffer "material or non-material damage" by reason of any contravention, by a data controller, of any requirements of the Data Protection Act 2018 (including the GDPR) are entitled to compensation for that damage. "Non-material damage" includes distress under the Data Protection Act 2018. This does not require the claimant to prove pecuniary loss.

Conspiracy. The economic tort of conspiracy requires there to be two or more perpetrators who are legal persons who conspire to do an unlawful act, or to a lawful act but by unlawful means.

Conversion is a tort that may cover unauthorised interference with personal information and other property.

Deceit. There are four elements: (i) the defendant makes a false representation to the claimant; (ii) the defendant knows that the representation is false, alternatively s/he is reckless as to whether it is true of false; (iii) the defendant intends that the claimant should act in reliance on it; and (iv) the claimant does act in reliance of the representation and in consequence suffers loss.

Directors' duties. See the answer to question 4.1.

Dishonest assistance may be claimed where there is a fiduciary relationship and dishonest assistance has been given by a third party to the breach of trust.

Infringement of copyright and/or database rights. Copyright is infringed when a person, without authority, carries out an infringing act under the Copyright, Designs and Patents Act 1988, such as copying the work or communicating the work to the public. Database rights are infringed if a person extracts or re-utilises all or a substantial part of a database without the owner's permission.

Misuse of private information. Similar to a breach of confidence, but removing the need for the claimant to establish a relationship of confidence. The cause of action may be better described as a right to informational privacy and to control dissemination of information about one's private life.

Negligence may be claimed where the defendant owed a duty of care to the claimant, breached that duty of care and that breach caused the claimant to suffer a recoverable loss.

Trespass is the intentional or negligent interference with personal goods. A deliberate attempt through the internet unlawfully to manipulate data on a computer may amount to trespass to that computer.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The following are illustrations of cases that have been brought that can be said to relate to Incidents.

Breach of confidence and various economic torts

Ashton Investments Ltd v OJSC Russian Aluminium (Rusal) [2006] EWHC 2545 (Comm): there was a good arguable case justifying service out of the jurisdiction, in respect of claims for breach of confidence, unlawful interference with business, and conspiracy where a computer server in London had allegedly been improperly accessed from Russia and confidential information and privileged information had been viewed and downloaded.

Contract

Bristol Groundschool Ltd v Intelligent Data Capture Ltd [2014] EWHC 2145 (Ch): a contract relating to the development of computer-based pilot training materials was a "relational" contract containing an implied duty of good faith. One party had behaved in a commercially unacceptable manner in accessing the other party's computer and downloading information, but its conduct was not repudiatory.

Frontier Systems Ltd (t/a Voiceflex) v Frip Finishing Ltd [2014] EWHC 1907 (TCC): an internet telephony provider's customer whose computer network had been hacked was not liable to pay the bill incurred by unauthorised third parties.

Trespass

Arqiva Ltd & Ors v Everything Everywhere Ltd & Ors [2011] EWHC 1411 (TCC): obiter reference to Clerk & Lindsell on Torts (20th Edition) at paragraphs 19-02 and 17-131. At paragraph 19-02, the authors state the proposition that "one who has the right of entry upon another's land and acts in excess of his right or after his right has expired, is a trespasser". At paragraphs 17-131 the authors refer to "Cyber-trespass" and say that "[w]hile the definition of corporeal personal property may normally be straightforward, questions may nevertheless arise in a number of borderline cases, in particular in respect of electronic technology. For example, it is hard to see why a deliberate attempt through the internet unlawfully to manipulate data on a computer should not amount to trespass to that computer".

Compensation for breach of the Data Protection Act 2018 (and GDPR)

Various Claimants v Wm Morrisons Supermarket PLC [2017] EWHC 3113 (QB) 2017: although determined under the previous legislation, in the first group litigation data breach case to come before the courts, Morrisons Supermarket was found to be vicariously liable for a deliberate data breach carried out by a rogue employee, out of working hours and at home on a personal computer. The ICO had, separately, concluded an investigation into the data breach and found that Morrisons had discharged its own obligations as required under the Data Protection Act 1998 and common law. The court concluded that Morrisons had no primary liability in respect of the breach, but there was nonetheless a sufficient connection (as the rogue employee accessed the data in question in the course of his employment) for Morrisons to have vicarious liability. Morrisons has been granted leave to appeal to the Supreme Court.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Please see the list in response to question 5.1.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Monitoring of employees, for example, monitoring use of email and internet access, involves processing of personal data and so the Data Protection Act 2018 (and the GDPR) will apply. The ICO's Employment Practices Code (the **Code**) contains guidance on monitoring employees at work. The Code states that employees still have an expectation of privacy, and so monitoring should be justified, proportionate, secured and that organisations should undertake an impact assessment and ensure that the employees are notified that monitoring will take place. This notification should include details of the circumstances in which monitoring will take place, the nature of the monitoring, how the information will be used and what safeguards are in place for the employees. A failure to comply with the Code will not automatically result in a breach of the Data Protection Act 2018. However, an organisation should be able to justify any departure from the Code, and the ICO can take this into account in consideration of any enforcement action.

Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, an organisation may lawfully monitor and record communications without consent to: (a) ascertain compliance with regulatory practices or procedures relevant to the business; (b) ascertain or demonstrate standards which ought to be achieved by employees using the telecommunications system; (c) prevent or detect crime; (d) investigate or detect unauthorised use of the telecommunications system (such as detecting a potential Incident); and (e) ensure the effective operation of the telecommunications system.

The Investigatory Powers Act 2016 amends some of the legislation relating to a business's ability to record telephone calls with its employees, but the operative provisions are not yet in force.

The Human Rights Act 1998, and in particular the right to respect for private and family life, home and correspondence, must also be considered and balanced against obligations on the organisation to implement appropriate security measures in respect of potential Incidents.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws which may prevent or limit the reporting of Incidents by an employee. However, the employee would need to satisfy the whistleblowing provisions in the Employment Rights Act 1996, one of which is that the subject matter of the disclosure falls into one or more of six categories. The categories include criminal offences and breach of a legal obligation, which may be appropriate for Incidents, although may not be wide enough to cover security flaws or mere risks.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have various surveillance powers under UK laws. For example, the Police Act 1997 authorises covert entry into and interference with communications systems by the police, and similar powers are available to the security services under the Security Service Act 1989 and the Intelligence Services Act 1994.

Other powers of surveillance and interception of communications data are subject to RIPA. Under RIPA, the Secretary of State can issue an interception warrant if this is necessary for the prevention or detection of serious crime (among others), provided this is proportionate and the information could not reasonably be obtained by other means. Under the Investigatory Powers Act 2016, new warrants are available for targeted equipment interference and targeted examination, as well as bulk warrants to enable law enforcement to obtain the communications data of multiple individuals using one warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under RIPA, telecommunications service providers are required to give effect to an interception warrant to assist law enforcement. The Secretary of State may issue a notice to a specified service provider detailing the measures that the service provider must implement to establish an interception capability.

The Investigatory Powers Act 2016 includes provision for the Secretary of State to require some telecommunications operators to install permanent interception capabilities through 'technical capability notices'. These notices will require approval by a Judicial Commissioner, but may include equipment interference, interception capability (such as removal of electronic protection applied to data) and disclosure of data. These provisions of the Investigatory Powers Act 2016 are not yet in force, but there is some uncertainty over whether these notices could prevent a telecommunications operator from providing end-to-end encryption capabilities to end users.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Alexandra Rendell is a senior associate specialising in commercial contracts, data protection, intellectual property and information technology law. Alexandra advises on complex commercial arrangements for a range of clients in the technology, life sciences and financial services sector, including outsourcing and service provision arrangements, licensing and IP/data exploitation.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 2639
Email: alexandra.rendell@allenovery.com
URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 15 partners with diverse backgrounds in data protection, bank regulation, anti-trust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity Incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

France

Frédéric Lecomte

Mélina Charlot

Stehlin & Associés

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is a criminal offence pursuant to article 323-1 of the French Criminal Code (FCC) relating to unauthorised access to an automated data processing system. The punishment for fraudulent access into an automated data processing system is imprisonment and a fine of up to €60,000. When data is modified or suppressed as a result of the unauthorised access, the sanction is three years of imprisonment and a fine of up to €100,000. When the offence is committed in a public or governmental system, the sanction is raised to five years of imprisonment and a fine of up to €150,000.

Denial-of-service attacks
Article 323-2 of the FCC sanctions the impeding or slowing down of an information system. Any kind of obstruction falling within the perimeter of article 323-2 is punishable by five years of imprisonment and a fine of up to €150,000. When the offence involves a public or governmental system, the sanctions are raised to seven years of imprisonment and a fine of up to €300,000.

Phishing
Phishing is sanctioned by the following articles of the FCC and of the Intellectual Property Code: (i) the collection of data by fraudulent, unfair or unlawful methods is sanctioned by article 226-18 of the FCC with five years of imprisonment and a fine of up to €300,000; (ii) the theft and use of a third-party identity is sanctioned by article 226-4-1 of the FCC by one year of imprisonment and a fine of up to €15,000 – the applied sanction is cumulative with the sanctions applied pursuant to (i) above; (iii) the fraud or swindle is sanctioned by article 313-1 of the FCC with five years of imprisonment and a fine up to €375,000; (iv) unauthorised introduction of data in a system, the extraction, reproduction, transmission and use of data stored in this system is sanctioned by article 323-3 of the FCC with five years of imprisonment and a fine of up to €150,000; and (v) phishing can result in an infringement of intellectual property rights, in particular on the basis of articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code. The owner of the reproduced or imitated website or trademark can sue the phisher for the use of his trademark on the basis of infringement. This offence is sanctioned with three years of imprisonment and a fine of up to €300,000.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This offence can by sentenced pursuant to article 323-1 of the FCC (*see Hacking*) but also pursuant to article 323-2 of the FCC (*see Denial-of-service attacks*) and pursuant to article 323-3 of the FCC (*see Phishing*).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Pursuant to article 323-3-1 of the FCC, the act consisting of, without a legitimate motive (in particular for research or computer security), importing, holding, offering, transferring or making available equipment, instruments, computer programs or any data designed or specially adapted to commit one or more offences mentioned in articles 323-1 to 323-3 of the FCC (*see Hacking, Denial-of-service attacks and Phishing*) is punished with the most severe sanctions.

Identity theft or identity fraud (e.g. in connection with access devices)
Pursuant to article 226-4-1 of the FCC, the act of usurping the identity of a third party is punishable by one year of imprisonment and a fine of up to €15,000.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The offence of theft pursuant to the FCC (article 311-1) has been extended to computer theft by French courts.

French judges now consider computer data (i.e. dematerialised information), as constituting goods likely to be stolen.

Under French law, theft is punishable by three years of imprisonment and a fine of up to €45,000.

Article 226-18 of the FCC as well as articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code (*see Phishing*) could also be used in some circumstances.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Article L.66 of the French Post and Electronic Communications Code imposes sanctions of two years of imprisonment and a fine of up to €3,750 for any person who, by breaking wires, damaging equipment or by any other means, deliberately interrupts electronic communications.

Attacks on the fundamental interests of the nation committed by means of information technologies are punished by numerous provisions of the FCC. For example, pursuant to article L.413-10 of the FCC, the destruction, misappropriation, subtraction, reproduction of the defence secrecy or the giving of access to an unauthorised person or making it available to the public, is sentenced to seven years of imprisonment and a fine of up to €100,000.

Failure by an organisation to implement cybersecurity measures
The failure by an organisation to implement cybersecurity measures does not constitute a criminal but an administrative offence, and the organisation would be subject to administrative fines and civil liability. Pursuant to the GDPR and the new French Data Protection Act (**FDPA**) n°78-17 of January 6, 1978 (amended by the GDPR), the administrative fine imposed by the French data controlling body (the CNIL) can be up to €20 million or 4% of the company's world-wide consolidated annual turnover.

Pursuant to Article 9 and 15 of the NIS Act, a manager that does not comply with required security measures even after the timeline specified in a formal request issued by the ANSSI (French national authority) may be sanctioned with a fine of €100,000 (for critical infrastructures) and €75,000 (for digital service providers).

1.2 Do any of the above-mentioned offences have extraterritorial application?

Pursuant to article 113-2-1 to the FCC, any crime or offence committed by means of an electronic communication network is deemed to have been committed on the territory of the Republic when it is attempted or committed to the detriment of a natural person residing in the territory of the Republic or a legal person whose registered office is in France.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

An offence will only be sanctioned by a court pursuant to the FCC if the intentional nature of the offence results from the facts or is demonstrated by the prosecutor. Pursuant to the GDPR as applied under French law, the lack of intentional motivation, all measures taken by the controller or the processor to mitigate the damage suffered by the data subjects, and/or the degree of cooperation to remedy the breach are considered as positive behaviour and may reduce the level of administrative sanctions.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Many of the FCC provisions may apply or be linked to cybercrime. For example, article 226-16 to 226-24 set out the criminal offences for the violations of the FDPA. With respect to terrorism, the following offences constitute acts of terrorism, when they are collectively or individually made to intentionally disrupt public order by intimidation or terror, the following offences: thefts; extortion; destruction; damage; and deterioration, including computer-related offences of the code (article 421-1 FCC). Moreover, article 421-2-5-1 of the same code sentences with five years of imprisonment and a fine of €75,000 the act of extracting, reproducing and intentionally transmitting data that intentionally promotes acts of terrorism.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The most important laws in the cybersecurity domain are (without being exhaustive):

- The Godfrain Law (*n°88-19 of January 15, 1988*).
- The FDPA (*Loi Informatique et Libertés n°78-17 of January 6, 1978*) successively amended by two laws: Law *n° 2004-575 of June 21, 2004* and finally amended by the *Law n°2018-793 of June 20, 2018* transposing the GDPR and the ordinance 2018-1125 of December 12, 2018.
- The Law for a Digital Republic *n°2016-1321 of October 7, 2016* and recently amended by the law transposing the GDPR (*Law n°2018-493 of June 20, 2018*).
- The Network and Information Systems Security Act ("**NIS Act**") transposing the NIS Directive *n°2018-133 of February 26, 2018* completed by the Decree *n°2018-384 of May 23, 2018* which details the application of the NIS Act and lists the sectors, types of operators and critical infrastructures concerned, and the Decree of September 14, 2018 defining the security rules (together the "**NIS Rules**").

In addition to the above-mentioned law, the following texts have adapted the criminal law to certain forms of cybercrime and creating specific investigative means such as:

- The Law on Daily Security (known as LSQ *n°2001-1062 of November 15, 2001*), *the Law on Internal Security* (*n°2003-239 of March 18, 2003*).
- The law adapting the judiciary to developments in crime (*n°2004-204 of March 9, 2004*), the Law on Copyright in the Information Society (known as *David's Law of August 1, 2006, n°2006-961*).
- The Law OPSI II (*n°2011-267 of March 14, 2011*).
- The Law strengthening the provisions on the fight against terrorism (*n°2014-1353, of November 13, 2014*).
- The Law strengthening the fight against organised crime and terrorism (*n°2016-731, of June 3, 2016*).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

In France, critical infrastructures identified as such by the law (*Law n°2013-1168 of December 18, 2013, Law n°2016-41 of January 26, 2016, NIS Act*) must comply with specific legal requirements. This is mostly the case for the following infrastructures:

- Professionals subject to the obligation of professional secrecy. For instance, pursuant to article 1111-8-2 of the French Public

Health Code, healthcare institutions as well as bodies and services carrying out prevention, diagnosis or care activities shall report without delay serious information system security Incidents to the Regional Health Agency.

- Operators for essential services ("**OES**") which, pursuant to the NIS Rules are designated by the Prime Minister in various sectors, such as Energy, Transportation, Banking, Financial Markets Infrastructures, Health, Digital Infrastructures. In that regard, the French NIS Rules added specific sectors to the list defined in the Directive such as: insurance; pharmaceutical retailing; and collective catering. The OES shall be designated by an order of the Prime Minister. The OES shall appoint a representative that will be the point of contact of the ANSSI. By November 2018, France had already identified 122 EOS.
- Digital service providers ("**DSP**"). Pursuant to the NIS Rules, these infrastructures must appoint a representative established on the national territory of the ANSSI if it is established outside the European Union and does not have any representative within the European Union.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Pursuant to the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the identified risk.

Pursuant to article 57 of the FDPA, the controller (and processor) are required to take all necessary precautions, having regard to the nature of the data and the risks associated with the processing, to preserve the security of the data and, in particular, to prevent it from being distorted, damaged or accessed by unauthorised third parties.

The NIS Rules also require OES and DSP to:

- carry out and maintain a list of networks and information systems necessary for the provision of the essential/digital services;
- identify the risks threatening the security of the information systems;
- guarantee an appropriate level of security according to the existing risks and implement technical and organisational measures necessary and proportionate to prevent, manage and reduce these risks;
- avoid Incidents and minimise their impact so as to guarantee the continuity of their services; and
- identify the IT security risks that may affect their activities.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Such conflicts may arise in France, for example, concerning the storage period of personal data (storage periods within the meaning of the FDPA may conflict with the rules of proof). Such conflicts may also arise with countries that are not a member of the European Union.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The GDPR (article 33) provides for an obligation for all data controllers to notify any Incidents to the competent data controlling body unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This notification to the data protection authority (CNIL) must take place within 72 hours of the discovery breach and must contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects, a detailed description of the measures taken to remedy or mitigate negative effects, the name and contact details of the data protection officer, and describe possible harmful consequences of the unlawful access and measures taken by the controller.

The FDPA (article 83) specifically concerns DSP and provides for an obligation to notify any data breach to the CNIL immediately and without conditions. The information to be communicated is rather similar to the above mentioned.

The NIS Rules also require OES and DSP to notify the ANSSI "without undue delay" any Incident when it has or is likely to have a significant impact on the continuity of services.

As regards the reporting procedures, organisations must provide the ANSSI by electronic means or by mail, with an Incident reporting form available on its website. This form includes information on the reporter, the network information system affected by the Incident, the consequences of the Incident on the services concerned, the type of Incident, its causes and the measures taken to respond to it.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

It is possible to voluntarily notify such security breaches to other competent authorities.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Pursuant to the GDPR and the FDPA, a controller must inform each affected individual of an Incident if the breach may create a high risk to the rights and freedoms of affected individuals (article 58 of the FDPA and 34 RGPD).

The information must detail the name and contact details of the data protection officer ("**DPO**") and describe in clear and plain language (i) the nature of the Incident, (ii) the likely consequences of the Incident, and (iii) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Pursuant to NSI Rules, OES and DSP only are required to report Incidents to the ANSSI.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

None of these cases would change the responses to questions 2.5 to 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The CNIL controls the proper application of the FDPA and the GDPR by data controllers and processors. It also gives opinions on legislative drafts or regulatory texts. The CNIL has important powers of control and investigation.

Finally, the CNIL has significant administrative and financial penalty powers and can take decisions such as the temporary or permanent suspension of data processing.

For application of the NIS Rules, the French National Cybersecurity Agency (ANSSI) is the national authority responsible for replying to cybersecurity Incidents targeting strategically important institutions (https://www.ssi.gouv.fr).

The Ministry of Defence and the Ministry of the Interior also assume functions of prevention of all forms of cybercrime.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Depending on the nature of the offence, the penalty may vary between €10 million or 2% of the worldwide turnover, and €20 million or 4% of the worldwide turnover.

OES and DSP may be subject to the following fines:

- €100,000 (€75,000 for DSP) in case of non-compliance with security rules.
- €75,000 (€50,000 for DSP) in case of failure to communicate a cybersecurity Incident.
- €125,000 (€100,000 for DSP) in case of obstruction of inspection operations.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Since the entry into force of the GDPR, the CNIL has sanctioned several companies. The CNIL fined Google LLC €50,000 for lack of transparency, unsatisfactory information and lack of valid consent for the customisation of advertising.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Insofar as beacons have the same purposes, and are deemed to be cookies, their use is legal provided such a use complies with cookie legislation.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

Under French law, loyalty of evidence production is material to the fairness of trial. Therefore, the law distinguishes between active and passive provocation to commit an offence. Honeypots should be considered as legal if used as passive traps to detect cyber threats. The French Cour de Cassation in a decision of 30 April 2014 stated that there had been no provocation to commit the offence in a case where the FBI had created a surveillance site to gather evidence of the commission of credit card fraud.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

Operating a sinkhole may not be compliant with the GDPR obligations insofar as some personal data could be collected without the consent of the computer's user and sent to the sinkhole. There is also a risk of collateral damage.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The measures to be implemented are stronger in some business areas. This is particularly the case for critical infrastructures which must comply with the NIS Rules (see question 2.2), or for Infrastructures that process sensitive data (for example, health data or data relating to criminal sentences, offences or security measures). Also, as mentioned above (see question 2.2), companies who host personal health data must be accredited for this purpose.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The legal requirements related to cybersecurity in the following two sectors are as follows:

(a) The financial services sector must comply with several requirements such as auditing IT systems, strengthening resistance to cyber risks, developing defences adapted to the complexity of cyber-attacks, and making several declarations to the ANSSI (ministerial orders of November 28, 2016).

(b) Pursuant to article L.33-1 of the French Post and Electronic Communications Code, companies in the telecommunication sector must comply with rules relating to the conditions of permanence, quality, availability, security and integrity of the network and service, which include obligations to notify to the competent authority breaches to the security or integrity of networks and services.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Beyond the company's responsibility in case of failure of the IT system (*see* question 2.10), the company manager (i.e. in France, it is the representative of the company who has the power to bind the company, e.g.: president; CEO; and general manager) is liable under civil law towards the company and its shareholders of (i) breach of the laws and regulations or of the bylaws, and (ii) mismanagement (article 1850 of the Civil Code). Moreover, the company manager can be liable because of the behaviour of his employees if such behaviour results in damage to a third party (article 1242 paragraph 5 of the French Civil Code). Finally, pursuant to the FCC and the French Commercial Code, numerous French provisions specifically make the company manager subject to personal criminal liability.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Please see below the Applicable Law requirements:

(a) There are no general obligations, so far, to designate a CISO. However, the GDPR sets out the obligation to appoint a DPO when (i) the data processing is carried out by a public authority or public body, (ii) the data processing requires regular and systematic monitoring on a large scale, and (iii) in cases of large-scale processing of sensitive data.

(b) For critical infrastructures, the NIS Rules set out the obligation to establish, maintain and implement a network and information system security policy ("**ISSP**"). The ISSP describes all procedures and organisational and technical means implemented by the operator to ensure the security of its essential information systems. The operator shall also maintain a crisis management procedure in the event of major cyber-attacks. For other companies, there are no general obligations to establish a written Incident response plan or policy.

(c) For critical infrastructures, the NIS Rules imposes on the OES to carry out and maintain a risk analysis of its essential information systems. Pursuant to the FDPA, the controller and the processor must carry out a risk assessment in order to implement measures to protect data processing systems. Moreover, pursuant to article 1110-4-1 of the French Public Health Code, health professionals, healthcare institutions and services must use information systems for the processing of health data, their storage on electronic media and their transmission by electronic means, in accordance with interoperability and security standards in order to guarantee the quality and confidentiality of personal health data and their protection.

(d) For critical infrastructures, the NIS Rules impose audits to assess the level of security of information systems with regard to known threats and vulnerabilities. For other companies, French law strictly applies the GDPR according to which the controller and the processor must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (article 32.1.d).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Pursuant to article L.225-100-1 of the French Commercial Code and article 222-3 of the General Regulations of the French Financial Markets Authority, listed and private companies must draw up an annual management report which contains a description of the main risks and uncertainties the company had to face or is facing (which implicitly includes cyber risks). Pursuant to article L.451-1-2 of the French Commercial Code, listed companies are required to submit this report to the French Financial Markets Authority and to publish it on their website.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

To the extent that they fall within the scope of the NIS Rules and/or the GDPR, public and listed companies are subject to the requirements of these texts.

In addition, public sector infrastructures are subject to the RGS (the general security database), which aims at securing electronic exchanges from the public sphere by ensuring that the level of security of these information systems is well adapted to the challenges and risks involved (article 1 of *Decree n°2010-112 of February 2, 2010*).

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Under French Law, the general rule of civil liability is set forth under article 1240 of the French Civil Code pursuant to which any act which causes damage to another shall oblige the person by whose fault it occurred to repair it (i.e. three elements are necessary to engage liability: (i) a fault; (ii) a damage; and (iii) a causal link between the two). Moreover, under the GDPR (article 79), a civil action may be brought in the event of an Incident if the controller or the processor have not complied with the GDPR requirements. Finally, under the FDPA, the data subject shall have the right to mandate a not-for-profit body, organisation or association to stop the breach and to obtain compensation (article 37).

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

For example, a woman was penalised in civil and criminal terms by the Chambery Court of Appeal on November 16, 2016 for the possession of hacking data.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

See the answers to questions 5.1 and 5.2.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber risk is partially covered by traditional insurance contracts which cover certain foreseeable consequences of certain computer threats (e.g. insurance contracts covering damage to property and civil liability). The emergence of new risks from the evolution of technologies and the increase in their uses requires the implementation of appropriate legal frameworks. To cope with these new risks, insurers have developed a new contract: the cyber contract; which is a multi-risk contract cover for damage (costs and losses incurred); liability (non-material damage to third parties); and management services of crisis.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Pursuant to article L.113-1 of the French Insurance Code, the insurer does not cover loss or damage resulting from the insured's intentional or wilful misconduct. In addition, criminal sanctions are not insurable because they are regarded as personal sanctions. Moreover, there is still a debate about the possibility to insure administrative or financial sanctions to the extent they are not the result of intentional misconducts. The authors opine that this risk should be insurable.

On the subject of terrorism and cyberterrorism, the French Public Purse stated that "*insurance contracts whose purpose is to guarantee the payment of a ransom to Daech, as to any terrorist entity, are prohibited*".

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The specific requirements under the Applicable Law are as such:

(a) The monitoring of employees is authorised. The employer can control and limit the use of the internet (site filtering devices, virus detection, etc.) and e-mail (tools for measuring the frequency of messages sent and/or the size of messages, "anti-spam" filters, etc.). The purpose of this control is to ensure the security of networks that could be attacked (viruses, Trojans, etc.) and to limit the risks of abusive or personal use of the internet or e-mail. However, (i) the introduction of a monitoring process to monitor employee activity requires prior information and consultation of the employee representative committee, and (ii) individual information for employees. As a consequence, the monitoring must be proportionate, i.e. respect the balance between the employee's private life and the employer's power of control.

(b) Except for the DPO, there is no specific statutory obligation for employees to report such risks to their employer. However, internal policies (such as company rules or an IT security charter) can encourage employees to adopt a proactive reporting behaviour if they noticed an Incident. In France, there is also a "whistleblowing" mechanism available to employees (this can be, for example, an "ethical line" telephone number or a specific e-mail address). This system enables employees to report problems that could seriously affect a company's activity or seriously engage its liability. However, this mechanism remains optional.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws that may prohibit or limit the reporting.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In France, there are many police services specialising in cybersecurity. For example: the PICyAN (Cybercrime investigation platform and digital analysis), which analyses IT equipment seized during police searches and internet surveillance thanks to special software; the C3N (Digital Crime Centre) whose mission includes judicial investigations and criminal intelligence; the BEFTI (Information Technology Fraud Investigation Brigade), which operates only in Paris and the surrounding suburbs and which is responsible for managing any breaches of the data processing system, software counterfeiting and classic offences such as fraud; and the OCLCTIC (Central Office for the Fight against Information and Communication Technologies Crime), which ensures the legality of published content on Internet and ordering providers to remove illegal content.

The police services mentioned above may carry out investigations, searches, interceptions, data collection, geolocation, wiretapping, infiltration, and arrest and detain suspects in police custody.

In addition, in order to ensure the effective application of the FDPA, the CNIL has the power to carry out extensive controls on all data controllers and processors. The ANSSI can also carry out controls on OES's facilities.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no obligation to set up backdoors. However, the administrative and judicial authorities may require the submission of encryption

keys. Pursuant to article L.871-1 of the French Internal Security Code, natural or legal persons who provide encryption services aimed at ensuring a confidentiality function are required to submit within 72 hours to authorised agents (i.e. administrative and judicial authorities) at their request, agreements enabling the decryption of data transformed by means of the services they have provided.

Frédéric Lecomte has been a member of the Paris Bar since 1989. Frédéric joined Stehlin & Associés in 1993 after having spent five years at Coudert Brothers in Paris. He became a partner in 1998.
Frédéric is the author of numerous articles in relation to technology law and is the author of a book about the GDPR *Nouvelle Donne Pour les Données* (Fauve Editions, 2018).
Practice areas: new technologies and data law; intellectual property; contract law and trade; and distribution law.

Stehlin & Associés
48 avenue Victor Hugo
Paris, 75016
France

Tel: +33 1 44 17 07 70
Fax: +33 1 44 17 07 77
Email: f.lecomte@stehlin-legal.com
URL: www.stehlin-legal.com

Mélina Charlot has been a member of the Paris Bar since 2017. Mélina joined Stehlin & Associés in 2019.
Practice areas: new technologies and data law; Intellectual property; Contract law and Trade; and distribution law.

Stehlin & Associés
48 avenue Victor Hugo
Paris, 75016
France

Tel: +33 1 44 17 07 70
Fax: +33 1 44 17 07 77
Email: m.charlot@stehlin-legal.com
URL: www.stehlin-legal.com

Stehlin & Associés is an independent business law firm that was founded in 1989.
The firm's attorneys work together in a pragmatic way to implement their projected operations and solve problems encountered by clients, both in their day-to-day business as well as in specific transactions. With an international outlook from the beginning of its existence, the firm has numerous contacts with firms throughout the world. Since 2012, the firm has been the French member of the Mackrell International network, which is ranked among the top law firm networks in *Chambers* 2018, having a presence in 60 countries and 170 cities, and providing access to more than 4,500 attorneys.
Our team assists its clients in the new technologies and intellectual property fields, which include copyright and neighbouring rights, industrial property rights, the internet and new technologies rights and privacy law.

www.stehlin-legal.com

Germany

Dr. Alexander Niethammer

Constantin Herfurth

Eversheds Sutherland

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking constitutes a criminal offence according to Sec. 202a of the German Criminal Code (so-called "unauthorised obtaining of data"). According to this provision, whosoever unlawfully obtains data for himself, or another, that was not intended for him and was especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.

Denial-of-service attacks
Denial-of-service attacks constitute a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data processing operation is of substantial importance for another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Phishing
Phishing can constitute two different criminal offences. The unlawful interception of data by technical means from a non-public data processing facility constitutes a criminal offence according to Sec. 202b of the German Criminal Code and is punishable with imprisonment for up to two years or a fine. The *use* of such data with the intent of obtaining an unlawful material benefit would constitute a criminal offence under Sec. 263a of the German Criminal Code (so-called "computer fraud") and is punishable with imprisonment for up to five years or a fine.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware constitutes a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data processing operation is of substantial importance to another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The sole possession of hardware, software or other tools which can be used to commit cybercrime can constitute a criminal offence according to Sec. 202c of the German Criminal Code. According to this provision, the preparation of the commission of an unauthorised obtaining of data or phishing by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible software for the purpose of the commission of such an offence shall be liable to imprisonment for up to one year or a fine. In case of a use of such instruments, the same principles as set forth above with respect to "Hacking" apply.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft can constitute various criminal offences, depending on how the offender obtains access to the identity data. This can either be done by phishing methods, which would constitute a criminal offence under Sec. 202b of the German Criminal Code, as set forth above with respect to "Phishing", or by use of such identity data for fraudulent purposes, which could constitute a criminal offence under Sec. 263 of the German Criminal Code (fraud) or Sec. 263a of the German Criminal Code (computer fraud), both are subject to imprisonment for up to 10 years.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft only constitutes a criminal offence under the preconditions of Sec. 202a of the German Criminal Code. Therefore, the affected data must be especially protected against unauthorised access. Usually, this is not the case when a current or former employee breaches confidence, as the employee has authorised access to the data. If this is not the case and the employee circumvents the protection, this would constitute the criminal offence of "phishing". The above-mentioned principles would apply.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Under German criminal law, some other activities in connection with the above-mentioned crimes constitute criminal offences. These are: (i) *preparing* of an unauthorised obtaining or interception of data, Sec. 202c of the German Criminal Code; (ii) handling of stolen data, Sec. 202d of the German Criminal Code; (iii) violation of postal and tele-

communications secrets, Sec. 206 of the German Criminal Code; (iv) computer sabotage, Sec. 303b of the German Criminal Code; (v) certain types of violation of the EU General Data Protection Regulation with the intention of enrichment or to harm someone, Art. 84 of the General Data Protection Regulation and Sec. 42 of the German Federal Data Protection Act; and (vi) falsification of digital evidence, Sec. 269 *et seq.* of the German Criminal Code.

Failure by an organisation to implement cybersecurity measures

The failure of an organisation to implement cybersecurity measures does not constitute a criminal but an administrative offence, and the organisation would be subject to civil liability in case of negligence. The financial penalty can be up to 10 million EUR or 2% of the company's annual turnover. The civil liability depends on the damage which occurred due to the organisation's failure and is basically not limited.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The above-mentioned offences have no specific extraterritorial application. However, the application of the German Criminal Code depends on the "place of the offence". According to Sec. 9 of the German Criminal Code, an offence is deemed to have been committed in every place where the offender acted or in which the result occurs, or should have occurred, according to the intention of the offender. Therefore, the above-mentioned offences will be applicable both if the offender acted in the territory of Germany and in case the offence affects IT systems which are situated or used for services provided in Germany where the offender acted from outside Germany.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, as a general principle, under German law, positive behaviour after a violation of a statutory provision, as well as compensation for the occurred damage, affect the level of penalties. However, this is at the sole discretion of the court.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

No, this is not applicable in our jurisdiction.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Cybersecurity is governed by several Acts in Germany. The main law relating to cybersecurity is the German IT Security Act (*IT-Sicherheitsgesetz*) of 25 July 2015, which amended a number of laws, in particular the German Telemedia Act (*Telemediengesetz*), the German Telecommunications Act (*Telekommunikationsgesetz*), the EU General Data Protection Regulation (*Datenschutz-Grundverordnung*), the German Federal Data Protection Act (*Bundesdatenschutzgesetz*) and the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*). Besides this, parts of cybersecurity are governed by the Banking Act (*Kreditwesengesetz*) and Securities Trading Act (*Wertpapierhandelsgesetz*). Besides this formal legislation, there are a few important informal provisions with respect to IT security in Germany. These are the BSI Basic IT Protection catalogues which are developed by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik – BSI*), the Common Criteria for Information Technology Security Evaluation, standardised as ISO/IEC 15408, and the Control Objectives for Information and Related Technology ("COBIT"). Furthermore, the European Cybersecurity Act provides the necessary authority to the European Union Agency for Cybersecurity ("ENISA") in order to establish a cybersecurity certification. Companies may voluntarily obtain such certification which is meant to inform the public about IT security provisions and general compliance with relevant IT security regulations. ENISA will perform cybersecurity trainings during which companies may evaluate their processes when being subject to a cyber-attack. Generally, the ENISA will be a principal contact for any cybersecurity-related questions.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Yes, the Act on the Federal Office for Information Security provides for specific obligations for providers of critical infrastructure. The law defines the following sectors as critical infrastructure:

- Energy.
- IT and Telecommunications.
- Transport and Traffic.
- Health.
- Water.
- Nutrition.
- Finance and Insurance.

However, not all companies acting in the above-mentioned sectors are subject to the regulations regarding critical infrastructure. These apply only *vis-à-vis* companies which are of great importance to the functioning of the community or which would cause a threat to public safety when having a supply shortfall.

Even though the Act on the Federal Office for Information Security provides for the obligation of providers of critical infrastructure to provide reasonable organisational and technical precautions to prevent disruption of the availability, integrity, authenticity and confidentiality of their information technology systems, the specific duties are not specified by the Act but are subject to guidelines on IT security set out by industry associations and approved by the Federal Office for Information Security.

The Network and Information Systems Directive has been implemented with effect from 30 June 2017.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, German and European law provide for several obligations for organisations to take measures to monitor, detect, prevent and mitigate Incidents.

In detail:

- According to Sec. 13, sub-sec. 7 of the Telemedia Act, telemedia providers are obliged to ensure that unauthorised access to related data is not possible. A telemedia provider in the Telemedia Act means, e.g., each operator of a website. The Telemedia Act does not provide details for measures that have to be taken by the provider. Specific requirements are, however, developed by the competent data protection authorities, e.g., with respect to the prevention of unauthorised access to websites, the data protection authorities request a SSL encryption of the related data.
- According to Sec. 109 of the German Telecommunications Act, providers of public telecommunications have to implement necessary technical measures to prevent phishing of personal data. Besides this, providers of public telecommunications are obliged to appoint a security officer and develop an adequate IT security model.
- Providers of several financial products are obliged to develop an IT-specific risk management (Sec. 25a of the German Banking Act (*Kreditwesengesetz*) and Sec. 80 of the German Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Art. 5 para. 1 (f) and Art. 32 of the General Data Protection Regulation, organisations are obliged to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This includes in particular:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical Incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures used for ensuring the security of the processing.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Such specific conflicts may arise with foreign laws with exterritorial reach.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, there are specific reporting obligations with respect to Incidents under German law.

In detail:

- There is a general obligation to notify security breaches to the competent data protection authority. This applies to any kind of personal data. An exception applies where the security breach is unlikely to result in a high risk to the rights and freedoms of the data subject (Art. 33 of the EU General Data Protection Regulation).
  The report must be made without undue delay and not later than 72 hours after having become aware of the breach, and has to contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects. The notification to the competent data protection authority must also describe possible harmful consequences of the unlawful access and measures taken by the body. The name and contact details of the data protection officer have to be provided as well.
- In case of a breach of critical infrastructure, as defined in the Act on the Federal Office for Information Security, the provider must notify the Federal Office for Information Security of any significant disruption to the availability, integrity and confidentiality of their information technology systems, components or processes which might lead to a breakdown or malfunction of the affected infrastructure.
- Providers of public telecommunications networks or services are obliged to report any IT breach to the Federal Network Agency. The report, which must be made immediately, has to contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Yes, there is no prohibition of such voluntary reports so long as possible (confidentiality) rights of third parties are safeguarded.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, in case of a security breach which creates a notification obligation (see above under question 2.5), the data subject must be notified as soon as (i) appropriate measures have been taken to secure the data or have not been carried out without undue delay, and (ii) a criminal enforcement is not/no longer at risk. The notification to the data subjects must describe the nature of the unlawful access and include recommendations for measures to minimise possible harm. Where notifying the data subjects would require unreasonable efforts, such notification may be replaced by a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Art. 34 General Data Protection Regulation). This obligation of notification applies provided the Incident is likely to result in a high risk to the rights and freedoms of the data subject. Further exceptions apply under Art. 34, para. 3 of the General Data Protection Regulation and Sec. 29 of the Federal Data Protection Act.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, none of these scenarios would change the responses to questions 2.5 to 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The requirements identified under questions 2.3 to 2.7 are enforced by the Federal Office for Information Security, competent Data Protection Authorities and the Federal Network Agency.

In detail:

- The Federal Office for Information Security is the main authority with respect to cybersecurity in Germany. This authority should be the main contact regarding questions about preventive security measures and is responsible for receiving notifications about security breaches with respect to critical infrastructures.
- Data Protection Authorities enforce all relevant data protection laws. In Germany, each federal state has a separate Data Protection Authority.
- The Federal Network Agency enforces the telecommunications-related laws and is responsible for receiving notifications about security breaches with respect to telecommunications networks and services.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Under the German IT Security Act, non-compliance may be subject to administrative fines of up to 100,000 EUR. Non-compliance with the mentioned requirements under the General Data Protection Regulation is subject to fines up to 10 million EUR or 2% of the worldwide annual turnover, whichever is higher.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

German data protection authorities started fining companies who have not complied with data protection laws. A German social network ("Knuddels") had to pay a fine of 20,000 EUR because it failed to properly secure users' data. Hackers managed to obtain 808,000 email addresses and almost two million usernames and passwords. These were stored unencrypted on the company's servers. Furthermore, the hackers obtained specific data as to the age and addresses of some users. As the social network immediately reported the security Incident, cooperated with the relevant data protection authority and made a high investment in new data security measures, the fine of 20,000 EUR was rather low. This was the first fine in Germany under the General Data Protection Regulation.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Yes, they are.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Yes, they are.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Yes, they are.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice with respect to information security in Germany mainly depends on the security relevance of the concrete business; in particular, whether the sector is considered as a sector which is related to critical infrastructures and whether the business processes sensitive personal data or not. However, there are no known sector-specific deviations from the strict legal requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes, in detail:

- Providers of certain financial products are obliged to develop an IT-specific risk management (Sec. 25a of the German Banking Act (*Kreditwesengesetz*) and Sec. 80 of the German Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Sec. 109 of the German Telecommunications Act, providers of public telecommunications have to implement the necessary technical measures to prevent phishing of personal data. Besides this, providers of public telecommunications are obliged to appoint a security officer and develop an adequate IT security model.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Yes, such failure may lead to a breach of directors' duties.

According to Sec. 130 of the German Administrative Offences Act (*Ordnungswidrigkeitengesetz – OWiG*), the owner or management of a company commits a misdemeanour if:

- it omits purposefully or negligently to appropriately control the company; and
- if a crime or misdemeanour was committed that could have been avoided or significantly impeded by exercising such control.

The obligation to control also includes the obligation to diligently select and monitor supervising personnel, active monitoring of the development of legal and technical standards, random inspections, enforcement of implementation measures, etc. The owner or management of a company is obligated to organise the company in a manner that allows the company to comply with the law. Consequently, failures to prevent, mitigate, manage or respond to an Incident can constitute a breach of directors' duties if the directors failed to implement the appropriate measures to avoid such occurrences.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There are no general obligations, so far, to either designate a CISO, establish a written Incident response plan or policy or conduct periodic cyber risk assessments. However, according to Art. 32 of the General Data Protection Regulation, such measures can be required in order to ensure appropriate IT security measures. Companies shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In particular, companies shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing. This has to be therefore assessed on a case-by-case basis. Furthermore, Sec. 109 of the German Telecommunications Act provides specific obligations for providers of public telecommunications.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Notification requirements generally exist solely with respect to security breaches (see question 2.5 above). However, with respect to publicly listed companies, sole cybersecurity risks without an Incident having occurred may trigger the obligation to disclose the cybersecurity risk in an *ad hoc* notification if the risk is likely to have an impact on the company's stock market price.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Companies are obliged to implement an IT security model. However, there are no detailed statutory provisions regarding such models.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The civil liability of a company depends on whether damage has occurred due to the organisation's failure to implement an appropriate IT security model. In this case, any individual or other company which suffered material damage can take civil actions against the company which is responsible for the Incident. This liability is basically not limited but can be covered by insurance.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The case law on Incidents in Germany is very rare due to the lack of the possibility of class actions in Germany.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes, civil liability in tort depends on the damage which occurred due to the organisation's failure and is basically not limited.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents and are common in Germany.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations to insurance coverage against any type of loss.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) Yes, the monitoring of employees is only permissible in specific cases, e.g., in case of definite suspicion. Comprehensive monitoring measures would not be admissible. In case of works-council representation, the monitoring of employees needs to be generally agreed in a works-council agreement.
(b) There is no specific statutory obligation for employees to report such risks to their employer. However, such obligations should be imposed on the employees by the employer's internal policies (e.g., whistle-blowing policies).

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

According to Sec. 5 of the German Trade Secret Law ("*Gesetz zum Schutz von Geschäftsgeheimnissen*"), information that constitutes a trade secret may only be disclosed by employees in order to report unlawful conduct or similar wrongdoing. A trade secret is any information that is not generally known, and subject to legitimate interest and appropriate safeguards to keep this information confidential.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Depending on the type of authority (e.g., Public Prosecutor, Federal Office for Information Security and Data Protection Authority), the enforcement powers vary. However, all authorities have the power to carry out on-site investigations including accessing IT systems.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No; so far, there is no such obligation. However, the German legislator is currently debating such an obligation with respect to social media and instant messaging accounts.

Alexander Niethammer is a Partner in the Munich office of Eversheds Sutherland and heads the Company Commercial Practice Group in Germany. He specialises in complex IT transactions, cybersecurity and data protection. Alexander has advised, for over 15 years, many Fortune 100 companies from the IT, industrials, consumer and financial sectors on global projects. He has a dual legal qualification as an attorney-at-law in New York (USA) and in Germany.
Alexander is recommended for Data Protection by *The Legal 500*, recognised as a leading IT lawyer by German business magazine *Wirtschaftswoche* and has been named by the International Law Office (ILO) as the exclusive recipient of the prestigious "Client Choice Award" as Germany's best IT & Internet counsel.

Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 318
Email: alexanderniethammer@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

Constantin Herfurth works as an Associate in the IT/IP practice at Eversheds Sutherland in Munich. His area of advice covers all aspects of data protection, IT law and cybersecurity. In particular, he has strong expertise in the management of data breaches. He mainly advises international and national clients from the diversified industries and health sector. In addition, he regularly writes for the specialist journals "*Zeitschrift für Datenschutz*" (journal for data protection) and "*MultiMedia und Recht*" (multimedia and law).

Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 295
Email: constantinherfurth@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

Eversheds Sutherland is one of the leading legal service providers in the world. Eversheds Sutherland represents the combination of two firms with a shared culture and commitment to client service excellence. We are each known for our commercial awareness and industry knowledge, and for providing innovative and tailored solutions for every client.
With 69 offices in 34 countries and more than 3,000 lawyers, we partner with many of the most dynamic and successful business organisations across Africa, Asia, Europe, the Middle East and the United States, to address their most critical challenges, support their legal needs and unlock their global ambitions.

Our international IT team with more than 100 members frequently works for major corporate and public clients across the globe, and also acts for some of the world-leading IT suppliers. Our cybersecurity practice spans the full range of data protection, cyber and information security law topics.

www.eversheds-sutherland.com

EVERSHEDS SUTHERLAND

Greece


Ioannis Giannakakis


Stefanos Vitoratos

G+P Law Firm

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking (i.e. unauthorised access) relating to information systems is a criminal offence pursuant to Ar.370C par.2 of the Greek Criminal Code (GCC), as it stands after the changes brought by Law 4411/2016, that nationally implemented the Budapest Convention on Cybercrime, carrying a penalty of imprisonment. If the action targets international relations or state security, it is sanctioned under Ar.148 GCC (espionage) which bears a penalty of life imprisonment if the data was used to damage the state (par.2). In case, due to hacking, the operation of an information system is severely hindered, it carries a penalty of up to three years of imprisonment (Ar.292B of GCC). When data is modified or suppressed as a result of unauthorised access, the sanction is up to three years of imprisonment as well (Ar.381A of GCC).

Denial-of-service attacks
Ar.292B of GCC sanctions the impeding of an information system's operation. Under the provisions of Ar.292B GCC, obstructions are punishable with up to three years of imprisonment. If a certain tool (hardware or software) was used for the attacks, the penalty varies from one to three years of imprisonment (Ar.292B GCC par.2 sec.a). Moreover, if the attack caused severe damage or targeted critical infrastructure, it is punishable with at least one year of imprisonment for each one of the cases respectively (Ar.292B GCC par.2 secs. b&c).

Phishing
Phishing can function as the basis for more than one criminal offences, punishable under the provisions of the Greek Criminal Code:

i. Under Ar.370D GCC, anyone who, with the use of technical equipment, proceeds with unauthorised monitoring, extraction or reproduction of a system's data, with the purpose of knowing its content, is sanctioned with up to 10 years of imprisonment. The same penalty for whoever uses the above-mentioned data (Ar.370D GCC par.2) and if the data is diplomatic or military (Ar.370D GCC par.3), faces the penalties of Ar.146 GCC under the title "state secrets violations", which provides imprisonment of up to 10 years.

Phishing as a preparatory action:

ii. Ar.292C sec.b of GCC carries a penalty of imprisonment of up to two years for whoever, in any manner, handles or sells passwords or access codes with the purpose of committing crimes sanctioned under Ar.292B GCC (impeding of an information system's operation).
iii. Ar.370E sec.b of GCC carries a penalty of imprisonment of up to two years for whoever, in any manner, handles or sells passwords or access codes with the purpose of committing crimes sanctioned under Ar.370B par.1 GCC (state and non-state secrets violation excl. diplomatic and military), Ar.370C par. 2&3 (unauthorised access) and Ar.370D (see under i).
iv. Ar.381B sec.b of GCC carries a penalty of imprisonment of up to two years for whoever, in any manner, handles or sells passwords or access codes with the purpose of committing crimes sanctioned under Ar.381A par. 1, 2 and 3 GCC (data damage).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This offence can be sanctioned pursuant to Ars.292B, 292C, 370C par.2, 370E, 381A, and 381B of the GCC as mentioned above under Hacking, Denial-of-service attacks and Phishing.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
This offence can be sanctioned pursuant to Ars.292C sec.a, 370E sec.a, 381A, and 381B sec.a of the GCC as mentioned above under Hacking, Denial-of-service attacks and Phishing.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft can constitute several criminal offences, depending on how and why the offender obtains access to the identity data. If phishing methods apply (see Phishing) and if such identity data is used for fraudulent purposes, it could constitute a criminal offence under Ar.386A of the GCC (fraud with the use of information system). The latter provides that, whoever, with the purpose of gaining illegal profit, damages foreign property by influencing through any means of data processing, faces the penalties of Ar.386 GCC, which provides for a penalty of up to 10 years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

i. There is no specific article in Greek Law containing "electronic theft", however, Greek courts have considered such offences under the provisions of Ar.386A GCC (fraud with the use of information systems) with the respective penalties (see above).
ii. Moreover, in Ar.370B GCC (state and non-state secrets violation excl. diplomatic and military), if the offender is offering its services to the data owner and the data has a great impact, then a penalty of at least one year of imprisonment is imposed (Ar.370B GCC par.2).
iii. In Ar.370C GCC (unauthorised access), if the offender is offering its services to the information system owner, the

offence is punishable only if it is expressly stated as such in the bylaws or in a written decision of the owner (Ar.370C GCC par.3).

iv. Last but not least, the Greek Law 2121/1993, regarding intellectual property, provides in Ar.65 for civil liabilities, and in Ar.65A for administrative penalties, up to 1,000 EUR/copy if someone reproduces and sells illegal copies. Moreover, Ar.66 of the same law imposes criminal penalties of at least one year imprisonment and a 2,900 EUR–15,000 EUR fine for any illegal unauthorised copy, reproduction and sale of material that are protected under its provisions.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The authors of the Greek Criminal Code have chosen a functional approach towards cybersecurity crimes and the articles have already been mentioned above. However, we should add that any attacks against the interests of the state, committed by means of information systems, are punished separately by numerous articles of the GCC. For instance, pursuant to Ar.370B GCC (state and non-state secrets violation excluding diplomatic and military) and according to par. 3, if the offence violates diplomatic or military secrets the offender faces the penalties of Ar.146 GCC (state secrets violations), which is imprisonment of up to 10 years and if he had no purpose in violating them, up to three years' imprisonment (Ar.147 GCC).

In Ar.370C par.2 GCC (unauthorised access), if the action targets international relations or state security (sec.2), it is sanctioned under Ar.148 GCC (espionage) which bears a penalty of life imprisonment if the data was used to damage the state (par.2).

In Ar.370D GCC, if someone, with the use of technical equipment, proceeds with unauthorised monitoring, extraction or reproduction of a system's data with the purpose of knowing its content, and this data refers to diplomatic or military secrets (Ar.370D GCC par.3), they face the penalties of Ar.146 GCC under the title "state secrets violations", which is imprisonment of up to 10 years.

Failure by an organisation to implement cybersecurity measures

The failure of an organisation to implement cybersecurity measures does not constitute a criminal but an administrative offence, meaning it would be subject to administrative fines and the respective civil liability.

Pursuant to Ar.83 of the GDPR and Ar.15 par. 6 of the newly voted Law 4624/2019, which implements certain aspects of the GDPR, the Hellenic Data Protection authority is competent to impose administrative penalties for failures related to data breaches. The financial penalty can be up to 10 million EUR or 2% of a company's annual turnover (Ar.83 par.4 GDPR), or even 20 million EUR or 4% of a company's annual turnover in Ar.83 par.5 GDPR, or can impose an administrative fine up to 10 million (10,000,000) EUR against any Public Authority (Ar.39 Law 4624/2019) as the latter is defined in Law 4270/2014.

Moreover, the Hellenic Authority for Communication Security and Privacy, in light of the provisions of Ar.11 of the Law 3115/2003 combined with those of Ar.19 of its No 205/2013 Act, named "Regulation for the Security and Integrity of Networks and Electronic Communications Services", has the authority to impose financial penalties from 15,000 EUR to 1.5 million EUR (Ar.11 sec.b Law 3115/2003) in case HACSP carries a scheduled or an own-motion review and finds severe lack of measures. However, in practice nothing dramatic has happened.

Last but not least the Law 4577/2018, which incorporates the NIS Directive EU 2016/1148, in Ar.15 par.1 sec.b, provides that the Minister of Digital Policy, Telecommunications and Media, following a recommendation from the Hellenic Cybersecurity Authority, may impose sanctions on 'operators of essential services' or 'digital service providers' that do not take appropriate and proportionate technical and organisational preventive measures for mitigating network and information systems security risks. These sanctions vary up to 50,000 EUR plus a recommendation to comply with the necessary provisions and a warning for further sanctions as a first stage (case b.aa), and in case of a repeated offence, he has the authority to impose sanctions of up to 200,000 EUR (case b.bb).

Regarding civil liability, it depends on the damage occurred due to insufficient cybersecurity measures and is not delimited.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The exact delimitation of the principle of territoriality is always a challenge when referring to cybercrimes. The Greek Criminal Code has chosen as a criterion for its application "the place of the offence" (Ar.5 par.1 GCC). As Ar.16 GCC provides, the "place of the offence" is where the offender actually committed the offence, in whole or in part, as well as the place where the result of the offence occurred, or, in the event of an attempt, the place that the result should have taken place according to the intention of the offender.

Moreover, Ar.5 par.3 GCC expressly states that when the offence is committed via a network or other means of communication, the Greek territory is also considered to be the "place of the offence" in case its territory provides access to the specific means, irrespective of the place of their primary establishment.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Any offence is only sanctioned by a court according to the GCC, depending on the intentional nature, the results and the facts that justify it. As a general principle, positive behaviour and the willingness to offer cooperation and compensation may reduce the penalties. Regarding the application of the GDPR under Greek Law, the lack of intention, the measures taken by the controller or the processor to mitigate the risk or damage suffered by the data subjects and the degree of cooperation to resolve the Incident are considered as positive behaviour. However, the level of penalty is left to the discretion of the court and to the competent authorities for the administrative part.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Many of the Greek Criminal Code provisions have been transformed by the Law 4411/2016, which nationally implemented the Budapest Convention on Cybercrime and may be linked to cybercrime, as mentioned above under the answer to question 1.1.

Moreover, after the latest changes brought to the Greek Criminal Code by the latest Law 4619/2019, the Code relates many offences with the use of the internet and information systems. Indicatively and not expressly we could refer to:

- Ar.135, which provides that "*Anyone, who publicly…or by the use of internet..intends or attempts to induce others to attempt acts of treason, shall be punished with up to ten years imprisonment*".
- Ar.183, which provides that "*Anyone, who publicly or via the internet, causes or stimulates civil disobedience, shall be punished with imprisonment of up to one year or with a fine*".

- Ar.184, which provides that "*Anyone, who publicly or via the internet, causes or stimulates serious offences, thus jeopardizes the public order, shall be punished with imprisonment of up to one year or with a fine*". Par.2 of the same article provides that "*if the above-mentioned offences are targeted at the perpetration of acts of violence against a certain group of people identified on the basis of racial characteristics, color, ethnic origin, ancestry, religion, disability, sexual orientation, identity or sex characteristics, the offender shall be punished with up to three years of imprisonment or with a fine*" and "*..if a crime is indeed committed, the imprisonment shall be up to five years*" (par.3). Finally, if the aim of the stimulation is to provoke violent acts in-between the people to disturb common peace "*the offender shall be punished with up to three years of imprisonment or with a fine*" (par.4).
- Ar.187A, with respect to terrorism, provides that "*Anyone, who publicly or via the internet threatens to commit an act of terrorism; or stimulates towards its conduct and thus jeopardizes the public order shall be punished with imprisonment of up to three years*".

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

There are several important laws in connection with the concept of cybersecurity, which are (without being exhaustive):

- The Law 4577/2018, which implements the NIS Directive (EU 2016/1148).
- The Law 4411/2016 which nationally implemented the Directive EU 2013/40 and the Budapest Convention on Cybercrime that accordingly transformed the Greek Criminal Code.
- The GDPR and the newly voted Law 4624/2019 that clarify certain national implementing measures regarding the Regulation and at the same time incorporates the LED (Directive EU 2016/680).
- The Law 4070/2012 regarding the organisation and operation of the electronic communications sector in Greece.
- The No 205/2013 Act of the Hellenic Authority for Communication Security and Privacy, named as "Regulation for the Security and Integrity of Networks and Electronic Communications Services", as published in the Greek Official Government's Gazzette on the 15th July 2013 No 1742.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Law 4577/2018 implements the NIS Directive (EU 2016/1148) and provides specific responsibilities for 'operators of essential services' (critical infrastructure). In Appendix 1, the Law refers to operators in the fields of energy, transportation, banking and finance, health, water and IT infrastructures. According to Ar.4 par.1, the Hellenic Cybersecurity Authority, in cooperation with the relevant regulatory authorities, is responsible for identifying the specific 'operators of essential services' and compiling a catalogue which should be renewed every two years (Ar.4 par.3 Law 4577/2018).

Moreover, pursuant to Ar.9 of Law 4577/2018, these operators must take certain technical and organisational measures to identify potential security risks, as well as to prevent and reduce the impact of Incidents when the latter occur. As Ar.10 provides, the Hellenic Cybersecurity Authority supervises their compliance with the provisions of the Law and, in case of severe misimplementation of the provisions, they may be subject to sanctions up to 200,000 EUR pursuant to Ar.15 of Law 4577/2018.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There are certain provisions of European and Greek law that provide for organisations' obligations to take measures to monitor, detect, prevent and mitigate Incidents:

- Pursuant to Ars.5 and 32 of the GDPR, the controller and the processor shall process data "*in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*" (Ar.5(f) GDPR) and "*shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*" (Ar.32 GDPR) including, among others, confidentiality, integrity, availability and resilience of IT systems.
- Pursuant to Ars.9 and 11 of the Law 4577/2018 that implements the NIS Directive, 'operators of essential services' (Ar.9) and 'digital service providers' (Ar.11) shall take appropriate and proportionate technical and organisational measures to mitigate the risks posed to the security of network and information systems that are necessary for their operations.
- The No 205/2013 Act of the Hellenic Authority for Communication Security and Privacy, named as "Regulation for the Security and Integrity of Networks and Electronic Communications Services", as published in the Greek Official Government's Gazzette (on the 15th July 2013 No. 1742), designates the technical and organisational measures to be taken by the providers of public communications networks or electronic communications services available to the public.
- According to Ar.37 par.7 of Law 4070/2012, regarding the organisation and operation of the electronic communications sector in Greece, the above-mentioned providers may be asked to provide information necessary to assess the security and integrity of their services and networks, including documented security policies to the Hellenic Telecommunication and Post Commission.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Potential conflicts may arise with laws of non-EU countries and with certain foreign laws with extraterritorial reach. Moreover, since all the above-mentioned legislation (under question 2.3) require separate notifications to be made to the respective competent authorities for a certain IT Incident or data breach, they can lead to a different evaluation of the same Incident, with ambiguous results.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There are several reporting obligations related to Incidents under European and Greek law:

Pursuant to Ar.33 of the GDPR, "*in case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach*" to the Hellenic Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification shall contain all the information referred to in Ar.33 par.3 (a–d).

The Law 4577/2018 that implements the NIS Directive provides, in Ars.9 par.1.c and 11 par.1.c, that in case of an Incident related to 'operators of essential services' (Ar.9 par.1.c) or to 'digital service providers' (Ar.11 par.1.c), the operators must notify without undue delay the Hellenic Cybersecurity Authority and the Hellenic CSIRT, including in their notification all the information necessary to identify the criticality of the Incident and its potential cross-border impacts. Certain measures should have been taken before any Incident occurs and a recovery plan should be in place beforehand.

Pursuant to Ar.17 par.2.d of the No 205/2013 Act of the Hellenic Authority for Communication Security and Privacy, named as "Regulation for the Security and Integrity of Networks and Electronic Communications Services", regarding the mitigation of any Incident that jeopardises the security and integrity of network and services, the provider shall, with undue delay, notify its relevant executives and the competent authorities (The Hellenic Authority for Communication Security and Privacy).

Pursuant to Ar.37 par.4 of the Law 4070/2012 regarding the organisation and operation of the electronic communications sector in Greece, organisations providing access to public communications networks or publicly available electronic communications services shall notify the Hellenic Telecommunication and Post Commission for any security breach or loss of integrity that may have a significant impact on the operation of the networks or services. The Commission in turn notifies the Hellenic Authority for Communication Security and Privacy according to Ar.37 par.8.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Pursuant to Ar.14 of the Law 4577/2018, any company, even if it is not identified as an "operator of essential services" and is also not a "digital service provider" as recognised in the context of the Law, can voluntarily report to the competent authorities any Incident that may have a significant impact on the continuity of its services.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Ar.34 of the GDPR provides that "*when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*" (par.1) and shall "*describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)*". The communication to the data subject is not required if any of the conditions of Ar.34 par.3 (a–c) are met.

The Law 4577/2018 that implements the NIS Directive provides, in Ars.9 par.4 and 11 par.5, that in case of an Incident related to'operators of essential services' (Ar.9 par.4) or to 'digital service providers' (Ar.11 par.5), the Hellenic Cybersecurity Authority, after consultation with the relevant provider, may inform the public of individual Incidents if informing the public is required to prevent a future event or to handle an ongoing Incident.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

None of the listed cases would change the responses to questions 2.5 to 2.7; however, certain confidentiality rights of third parties should always be safeguarded.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The requirements referred to under questions 2.3 to 2.7 are enforced by the competent authorities below:

- The Hellenic Data Protection Authority is a constitutionally consolidated Independent Authority and was established by Law 2472/97, and now its authority has somewhat been extended by the newly voted Law 4624/2019.
- The Hellenic Authority for Communication Security and Privacy has been established under Law 3115/2003 and Ar.19 par.2 of the Hellenic Constitution. It has, among others, the duty to put into effect scheduled and emergency auditing procedures, *ex officio* or upon complaint, to examine complaints regarding the protection of the applicants' rights and to proceed in monitoring the compliance to the terms and the procedures of waiving off communication privacy.
- The Hellenic Telecommunications and Post Commission is an Independent Authority that acts as the national regulator that

monitors, regulates and supervises: (a) the electronic communications market, within which fixed and mobile telephony, wireless communications and Internet access providers operate; and (b) the postal services market, within which postal and courier service providers operate. The Authority was established in 1992 by virtue of Law 2075/1992, however, several new laws and amendments have expanded its competences. The Laws in force are 4070/2012 and 4053/2012.

- The Hellenic Cybersecurity Authority (HCA), as designated by Ar.7 of the Law 4577/2018 that implements the NIS Directive, is the Directorate of Cyber Security of the General Secretariat of the Ministry of Digital Policy, Telecommunications and Media (as established by Ar.15 of the decree 82/2017). Among other duties, the HCA monitors the implementation of the Directive, cooperation with the Hellenic CSIRT and is designated as the single point of contact exercising a liaison function to ensure cross-border cooperation with competent authorities of other EU Member States.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

According to Ar.83 par.4.a, the penalty, i.e. administrative fine, amounts to up to 10 million (10,000,000) EUR or in case of an undertaking up to 2% or the total worldwide turnover of the preceding financial year, whichever is higher. Moreover, according to Ar.39 of the newly voted Law 4624/2019, which implements certain aspects of the GDPR, the Supervisory Authority, i.e. the Hellenic Data Protection Authority, can impose an administrative fine up to 10 million (10,000,000) EUR against any Public Authority as the latter are defined in Law 4270/2014, amongst others, for violations of Ars.33–35 of the GDPR for not reporting an Incident or not informing the affected data subjects.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No enforcement action has been taken in Greece based on Ar.83 par.4.a of the General Data Protection Regulation up to date.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The use of beacons is not explicitly prohibited in Greece. However, their use would require prior explicit information of the data subject using the equipment containing the beacon.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
The use of honeypots is permitted in Greece.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Please see previous answer, i.e. the use of sinkholes is permitted.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

General market practice with respect to information security in Greece varies amongst regulated and non-regulated sectors of the economy. Regulated sectors, e.g. Telecommunications, Health and Technology Providers usually follow stricter industry standards, i.e. ISO/IEC 27001, 27005 and 37001, to safeguard the integrity, availability, confidentiality and resilience of their information systems.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

There are no sector-specific legal requirements in relation to cybersecurity applicable to organisations in the financial services sector and regarding the telecommunications sector, there are only minimal provisions that have been mentioned above, mainly Ar.37 of Law 4070/2012 regarding the organisation and operation of the electronic communications sector in Greece. Both sectors, however, fall under the Laws 4411/2016 and 4577/2018, along with the rest of the organisations in various industry sectors.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

According to Law 4577/2018, which incorporates the NIS Directive into Greek legislation, only "Critical Infrastructure Providers", i.e. Operators of Essential Services (OES) in the fields of energy, transport, credit institutions, financial market infrastructure, health, water supply and digital infrastructures. Providers of Digital Services (DSP), in particular e-commerce businesses and in general, digital services, search engines and cloud computing providers, are subject to administrative fines imposed against the legal entity and the natural persons (individuals), i.e. directors or employees of the aforementioned legal entities. However, there is no specific Applicable Law regulating that a failure by the legal entity to prevent, mitigate, manage or respond to an Incident amounts to a breach of directors' duties.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Companies, with the exception of Operators of Essential Services (OES) and Providers of Digital Services under the definition of Law

4577/2018 and the NIS Directive, are not legally required by any Applicable Law to designate a CISO, establish written Incident Response Plan or conduct Periodic Risk Assessments, including Third Party Vendors and performing penetration tests or vulnerability assessments. However, the prevailing interpretation of Ar.32 of the General Data Protection Regulation (Reg 2016/679 EU) includes the Incident Response Plan or Policy, the risk assessments and the periodic penetration tests in the appropriate technical measures that Data Controllers and Data Processors need to take to comply with the critical obligation of secure personal data processing. The designation of the CISO is mentioned in standards ISO/IEC 27001 and 22301 and is recommended, not mandatory, for companies abiding by the aforementioned information security standards.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

According to Ar.9 of Law 4577/2018 (incorporating into Greek internal legislation NIS Ar.14), Operators of Essential Services and Providers of Digital Services under question 4.1 shall notify, without undue delay, the Hellenic Cybersecurity Authority and the CSIRT of Incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the Incident. Notification shall not make the notifying party subject to increased liability.

In order to determine the significance of the impact of an Incident, the following parameters in particular shall be taken into account:

(a) the number of users affected by the disruption of the essential service;
(b) the duration of the Incident; and
(c) the geographical spread with regard to the area affected by the Incident.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are no further or additional specific requirements applicable to companies under Applicable Laws in relation to cybersecurity, apart from the ones mentioned in Law 4577/2018 related to Operators of Essential Services and Providers of Digital Services.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Ars.79 and 82 of the General Data Protection Regulation provide for the right of any affected data subject, i.e. individual that has suffered material or non-material damage as a result of an Incident, i.e., in this case, a Personal Data Breach to seek compensation from the Data Controller or Data Processor. In this case the Incident shall be a hack or any violation or threat to the confidentiality, integrity and availability of the data subject's Personal Data that resulted in a material or non-material damage to the data subject. A critical element of the lawsuit is the evidence and proof of the damage, or the data subject, as a result of the Data Breach, i.e. Incident.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Decision 7/2019 of the Hellenic Data Protection Authority imposed a fine to HELLENIC PETROLEUM GROUP for illegal processing of personal data and inadequate implementation of organisational and technical measures that resulted in the leak of special categories personal data.

Decision 85/2015 of the Hellenic Data Protection Authority against OLYMPION HOTEL SA, for not taking adequate organisational and technical measures to safeguard the security of its information systems that resulted in a data breach (Incident in the form of unauthorised access to personal and special categories data).

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

According to Ar.79 of the General Data Protection Regulation and Ar.67 of the new draft legislation, there may be liability in tort for the Data Controller in case a data subject suffers material or non-material damage from acts or omissions of the Data Controller that violate the Regulation, or any Member State national legislation, and is obliged to compensate the data subject for any such damage suffered.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out Cyber Privacy Insurance Coverage in Greece.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration. The coverage is decided by the insurance company and its underwriters, who can provide coverage to everything that is insurable by law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The new Greek Law 4624/2019 allows the use of monitoring systems, including CCTV cameras, for the purpose of preventing,

detecting and mitigating criminal offences and other violations conducted by employees in work, and does not explicitly refers to responding to Incidents nor to reporting of cyber risks or security flaws by employees to their employer. However, since a Data Breach can consist an Incident, the prevention, detection and mitigation of the latter falls under the interpretation of monitoring employees for the aforementioned purposes. The use of any monitory system or facility needs to take into account the principle of proportionality and accountability with regard to the collection and storage of employees' personal data whilst the maximum storage period is limited to 15 calendar days (with the exception of longer storage of up to three months in case of the detection or mitigation of criminal offences).

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There is no national legislation or any Applicable Laws prohibiting or limiting the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee to the employer.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Cyber Crime Unit of the Hellenic Police and the newly established Hellenic Cybersecurity Authority, along with the Hellenic Data Protection Authority and the Hellenic Authority for Communication Security and Privacy, are the key Authorities in Greece relied upon for the investigation of an Incident. All aforementioned law enforcement Authorities have extensive investigatory powers to conduct ordinary and extraordinary audits, *ex officio* or following a complaint, and impose administrative fines and criminal sanctions to individuals and legal entities of the public and private sectors in Greece.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no sector-specific or otherwise explicit requirements for organisations to implement backdoors in their IT systems for law enforcement authorities or provide law enforcement authorities with encryption keys. However, during an audit by any Authority, the provider or organisation under audit is obliged to cooperate in any possible way with the Auditing Authority and, if so requested, to also provide encryption keys to the auditors for specific audit purposes.

Ioannis Giannakakis is a Data Protection and Cybersecurity Thought Leader in Greece, being the number one internationally certified Greek Data Protection Officer in the world. Ioannis is the only Legal Counsel in Greece designated as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and holder of multiple other international Privacy Certifications (CIPP/E, CIPP/US, C-DPO and C-GDPR P). Ioannis co-founded the DPO Academy (www.dpoacademy.gr), the leading Education Management Organisation in Greece, having trained more than 60% of the Data Protection Officers in Greece and has published many scientific articles in various jurisdictions.
Ioannis has led as Project Leader in more than 22 GDPR Compliance Projects in Greece and the EU, and currently offers his services as Data Protection Officer to many large Greek companies. Last but not least, Ioannis has been selected by the Hellenic Cybersecurity Authority as the leading Cybersecurity & Legal Expert to assist the HCA in implementing the NIS Directive and suggesting the Audit and Penalties Procedure into Greek Executive Law (L4577/2018).

G+P Law Firm
60A Skoufa Street 10682
Athens
Greece

Tel: +30 216 80 90 074
Email: john.giannakakis@gplawfirm.eu
URL: www.gplawfirm.eu

Stefanos Vitratos is a Data Protection and Cybersecurity Expert Lawyer who graduated from Athens Law School and is a holder of two more post-graduate degrees, one in International Financial Law and one in International Politics.
He has previously worked as a consultant with several Law Firms in Athens, as well as for the Permanent Representation of Greece to NATO and the Embassy of Greece in the United Kingdom. In addition, he is Co-Founder of Homo Digitalis, the first digital rights NGO in Greece.
Lately, he is involved with regulatory compliance technologies business that can be put to the service of citizens, with the ultimate goal of always creating a culture of data protection, cybersecurity and human rights protection as a whole. He speaks fluent English, French and German.

Homo Digitalis
17 Agniadon Ave,118 54
Athens-Rouf, Attica
Athens
Greece

Tel: +30 210 25 32 938
Email: stefanos.al.vitoratos@gmail.com
URL: www.homodigitalis.gr

India


GV Anand Bhushan


Tejas Karia


Shahana Chatterji

Shardul Amarchand Mangaldas & Co.

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

- Section 43 of the Information Technology Act 2000 ("IT Act") provides that if any person accesses a computer, computer system or computer network without permission of the owner, or downloads, copies and extracts any data, or causes disruption of any system; *inter alia*, they will be liable to pay damages by way of compensation to the person so affected. The offence of hacking is covered under the above-described acts.
- Section 66 of the IT Act provides that if any person, dishonestly or fraudulently, commits any act referred to in Section 43, it will be punishable with imprisonment for a term of up to three years or with a fine of up to five lakh rupees (~USD 7,210), or with both.

For examples of prosecution, please refer to question 5.2.

Denial-of-service attacks

- Causing denial of access to any person authorised to access a computer network or resource is punishable under Section 43(f) of the IT Act with imprisonment for a term of up to three years or with a fine of up to five lakh rupees (~USD 7,210), or with both.
- Additionally, the crime of cyber terrorism under Section 66F specifies that whoever has the intent to threaten the unity, integrity, security or sovereignty of India, or to strike terror among people, denies or causes denial of access to any person authorised to access computer resource, will be punished with imprisonment of up to imprisonment for life.

Phishing

- Section 66C of the IT Act could be used to prosecute a person for phishing attacks. It provides that whoever, fraudulently or dishonestly, makes use of the electronic signature, password or any other unique identification feature of any other person, will be punished with imprisonment of up to three years and will also be liable to a fine of up to one lakh rupees (~USD 1,442).
- Additionally, Section 66D of the IT Act provides that whoever uses a computer resource for cheating by personation will be punished with imprisonment of up to three years and will also be liable to a fine of up to one lakh rupees (~USD 1,442).
- Section 74 provides punishment for knowingly creating or publishing an Electronic Signature Certificate for any fraudulent or unlawful purpose. The person in question will be punished with imprisonment for a term of up to two years or with a fine of up to one lakh rupees (~USD 1,442), or with both.

For examples of prosecution, please refer to question 5.2.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

- Section 43 of the IT Act provides that if any person introduces any computer contaminant or computer virus to a computer resources without the owner's permission will be liable to pay damages by way of compensation to the person so affected, and may also be punished with imprisonment for a term of up to three years or with a fine of up to five lakh rupees (~USD 7,210), or with both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Mere possession of such tools is not criminalised specifically. However, Section 66B of the IT Act provides punishment for dishonestly receiving stolen computer resources or communication devices, which may lead to imprisonment of up to three years and a fine of up to one lakh rupees (~USD 1,442).

Furthermore, any such tools used to commit a cybercrime may be confiscated under Section 76.

Identity theft or identity fraud (e.g. in connection with access devices)

- Section 66C of the IT Act provides penalties for fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person. Such a person will be punished with imprisonment of up to three years and a fine of up to one lakh rupees (~USD 1,442).
- Section 419 of the Indian Penal Code 1860 provides punishment of imprisonment for up to three years or a fine, or both, for cheating by personation. Section 66D specifically provides for the offence of cheating by personation using a computer resource. This attracts imprisonment of up to three years and a fine of up to one lakh rupees (~USD 1,442).

- Example of prosecution: In the case of *CBI vs. Arif Azim* in 2003, Sony India Private Limited operated a website enabling NRIs to send Sony Products to their friends/relatives in India after paying for it online. An individual gained access to the credit card number of an American national and ordered Sony Products by using her identity. He was convicted under Section 419 of the Indian Penal Code 1860.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

- Section 72 of the IT Act provides for breach of confidentiality and privacy. It provides that if any person who has access to any electronic record, document or other material, without the consent of the person concerned, discloses such document or other material to any other person, they will be punished with imprisonment of up to two years or with a fine of up to one lakh rupees (~USD 1,442), or with both.
- Section 72A of the IT Act provides that any person who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, discloses the same without consent, or in breach of the lawful contract, knowing it is likely to cause harm, will be punished with imprisonment for a term of up to three years or with a fine of up to five lakh rupees (~USD 7,210), or with both.
- Section 409 of the Indian Penal Code 1860 provides for punishment of imprisonment, and a fine, for criminal breach of trust by a public servant or agent. Section 420 of the Indian Penal Code 1860 provides punishment for cheating. Section 379 of the Indian Penal Code 1860 provides punishment for theft. All these Sections can also be invoked in case of electronic theft.
- Section 63 of the Copyright Act 1957 provides punishment for copyright infringement, leading to imprisonment for a period not less than six months but up to three years, and with a fine not less than 50 thousand rupees (~USD 721) but up to two lakh rupees (~USD 2,382).
- Example of prosecution: In the case of *Gagan Harsh Sharma and Others v. State of Maharashtra and Ors.* (2019 ALL MR (Cri) 595), an employee was accused of stealing software developed by his company. The accused had already been punished under Sections 420, 408 and 379 of the Indian Penal Code 1860, which provide punishment for the offences of cheating, criminal breach of trust by a servant and theft. The court did not allow an action under Section 66 of the IT Act on the grounds that to prosecute them under Section 66 would be a violation of the protection against double jeopardy.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

- Concealment or destruction of source code – Section 65 of the IT Act provides that whoever knowingly or intentionally conceals or destroys any computer source code when it is maintained by law for the time being in force, will be punishable with imprisonment of up to three years or with a fine of up to two lakh rupees (~USD 2,382), or with both.
- Securing access or attempting to secure access to a protected system – Section 70 of the IT Act authorises the appropriate government to declare a computer resource as a protected system and prohibit its access by the general public. Securing access or attempting to secure access to a protected system imposes imprisonment of up to 10 years with a fine.

Failure by an organisation to implement cybersecurity measures

- Section 43A of the IT Act provides uncapped compensation for failure to take adequate measures to protect any sensitive personal data or information held by a body corporate in a computer resource which it owns, controls or operates.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All offences under the IT Act have extraterritorial application to the extent that they are committed using a computer resource or network located in India.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

No mitigation strategies are set out in law.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Cyberterrorism is a specifically defined offence under Section 66F of the IT Act, which may attract imprisonment for life. The conditions of the offence are as follows:

a. the offence must be committed with the intent to threaten the unity, integrity, security or sovereignty of India, or to strike terror in the people;
b. it may constitute any of the following acts: *(i)* denying access to any person authorised to access a computer resource; *(ii)* attempting to penetrate or access a computer resource without authorisation, or exceeding authorised access; or *(iii)* introducing or causing to introduce any computer contaminant to a computer; and
c. by means of such conduct, the perpetrator causes or is likely to cause death or injuries to persons, damage/destruction of property, disruption of supplies or services essential to the life of the community or adversely affects the critical information infrastructure.

The offence may also be triggered if the perpetrator knowingly or intentionally accesses a computer resource, without authorisation, and obtains access to information, data or a computer database that is restricted for reasons of security of the State or foreign relations.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

In India, the horizontally applicable cybersecurity measures are provided for in the IT Act and the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 ("**CERT-In Rules**") thereunder.

The CERT-In Rules require individuals and corporate entities affected by certain types of "cybersecurity incidents" to mandatorily report the same to the CERT-In for the purpose of obtaining assistance.

Specific security-related compliances for certain types of information are also found in the following:

a. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**").
b. Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 ("**Protected System Rules**").
c. Companies (Management and Administration) Rules, 2014 ("**CMA Rules**").

In addition to this, there are sectoral cybersecurity related compliances applicable to regulated entities such as banks and NBFCs. Please refer to question 3.2 for these.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Under Section 70 of the IT Act, the Government may notify any computer resource which affects the facility of Critical Information Infrastructure ("**CII**") to be a "protected system". CII refers to a computer resource where the incapacitation or destruction of which can have a debilitating impact on national security, economy, public health or safety.

One example of a "protected system" notified under this law is the UIDAI-CIDR, which is a centralised database of all Aadhaar numbers (a centralised identification number) and other identification details of all Indian users.

Under the Protected System Rules, there are specific cybersecurity practices to be followed by an organisation having a "protected system". An illustrative list of these requirements are as follows:

a. the organisation should constitute an Information Security Steering Committee to approve all information security policies pertaining to the "protected system" and designate a Chief Information Security Officer ("**CISO**");
b. the CISO should co-ordinate with the National Critical Information Infrastructure Protection Centre (the Government's nodal agency in respect of critical infrastructure protection) in respect of cybersecurity Incidents and incorporate inputs suggested by the latter;
c. all Incidents should be communicated to the committee in a timely manner;
d. information security audits and compliances related to the "protected system" should be shared with the committee;
e. information system management practices should be continuously monitored and updated in accordance with central government guidelines;
f. control access to systems and maintain regular backups and logs; and
g. conduct periodic audits of systems.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There are no general cybersecurity requirements applicable on all sectors with regard to monitoring, detecting and mitigating Incidents. However, particular obligations exist in specific cases:

a. **When dealing with sensitive personal information of natural persons** (financial and health information, password, biometric data, etc.) – As per the SPDI Rules, all companies storing such data should have information security systems in place that are commensurate to the information assets sought to be protected. They should be compliant with ISO 27001, or equivalent standard certifications, and undergo periodic audits.
b. **For companies, when dealing with electronic records** – As per the CMA Rules, companies should ensure the security of any electronic records, including: protection against unauthorised access; alteration; tampering; maintaining the security of computer systems, software and hardware; protecting signatures; taking periodic backups; etc.
c. **For companies with "protected systems"** – For organisations which have any computer resources notified by the Government as a "protected system" (see question 2.2 above), the Guidelines for Protection of Critical Systems by the National Critical Information Infrastructure Protection Centre would have to be followed by the CISO and the network architecture should be stable, resilient and scalable.
d. **For listed companies governed by SEBI** – Such companies should have a Risk Management Committee as per the CMA Rules, meeting at least once a year and covering within its mandate cybersecurity risks.
e. **For banks / NBFCs** – The Reserve Bank of India ("**RBI**") notification on Cyber Security Framework for Banks includes obligations to put in place a dedicated cybersecurity policy which includes a mechanism for dealing with and reporting Incidents, have a cyber crisis management plan, arrange for continuous surveillance of systems and protect customer information. A similar framework exists in respect of NBFCs.
f. **For insurers** – The Insurance Regulatory and Development Authority of India ("**IRDAI**") has issued Guidelines on Information and Cyber Security for Insurers which include the designation of a CISO and the formulation of a cyber crisis management plan.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

There does not appear to be any conflict of law issue that arises in this context. However, law enforcement access requirements include handing over any information requested in a format accessible to the government, including in decrypted form where applicable. In principle, this may conflict with certain privacy protective measures employed by companies.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The CERT-In Rules require individuals and corporate entities affected by certain types of 'cybersecurity incidents' to mandatorily report the same to the CERT-In.

The reporting obligation is triggered with respect to the following kinds of Incidents:

a. targeted scanning/probing of critical networks/systems;
b. compromise of critical systems/information;
c. unauthorised access of IT systems/data;
d. defacement of website, or intrusion into a website, and unauthorised changes such as inserting malicious code, links to external websites, etc.;
e. malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware;
f. attacks on services such as Database, Mail and DNS, and network devices such as Routers;
g. identity theft, spoofing and phishing attacks;
h. Denial of Service ("**DoS**") and Distributed Denial of Services (DDoS) attacks;
i. attacks on critical infrastructure, SCADA Systems and Wireless networks; and
j. attacks on applications such as E-Governance, E-Commerce, etc.

The reporting authority in this regard is the Indian Computer Emergency Response Team ("**CERT-In**").

The CERT-In Reporting Form (here) specifies the kind of information to be provided, and includes:

a. the sector in question;
b. physical location of the affected computer;
c. time and date of incident;
d. type of incident;
e. information on affected system;
f. description of incident;
g. IP address;
h. details of security infrastructure; and
i. other details, including additional information voluntarily provided.

Separate reporting requirements exist in respect of cybersecurity incidents in regulated sectors. For instance, banks have to report cybersecurity incidents to the RBI within two-six hours, and insures to the IRDAI within 48 hours.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

In addition to the mandatory categories of information specified in question 2.5, it is possible for companies to report any other cybersecurity incidents to the CERT-In and seek assistance in this regard.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

No such general requirements exist.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The different regulators and supervisory authorities responsible for enforcing the above requirements are as follows:

a. Indian Computer Emergency Response Team.
b. Reserve Bank of India.
c. Insurance Regulatory and Development Authority of India.
d. National Critical Information Infrastructure Protection Centre.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

In general, failure to make reports to CERT-In may attract penalties in the form of fines up to 25,000 rupees under Section 45 of the IT Act. Non-compliance with directions of CERT-In may also attract criminal penalties under Section 70B of the IT Act, with imprisonment of up to one year or fines up to one lakh rupees, or both.

Separate action may be taken by regulators in respect of specific sectoral reporting requirements.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As far as CERT-In reporting is concerned, no specific enforcement trend has emerged in this respect.

In other instances of violation of enforcement action – The RBI has imposed, by an order dated July 31, 2019, monetary penalty of one crore rupees (USD 141,030) on Corporation Bank for non-compliance with the directions issued by RBI on (i) Cyber Security Framework in Banks, and (ii) Frauds Classification and Reporting by commercial banks.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no specific law in this regard, and such measures may be taken if they do not attract liability under any of the cyber offence provisions in law.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Please see above.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Please see above.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, the requirements are more stringent for the more highly regulated sectors such as the financial sector and the telecommunications sector. Please see details in question 3.2 below.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial Sector
Regulated entities such as banks, NBFCs and insurance companies are subject to a higher standard of cybersecurity measures than other entities, as there are sectoral regulations applicable to them.

An illustrative list of regulations imposed by the RBI on banks and NBFCs is provided below:

a. Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, 2006: guidelines on outsourcing; specifying what functions can be outsourced and what cannot; and security measures to be maintained (for banks).
b. Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs, 2017: guidelines on outsourcing; specifying what functions can be outsourced and what cannot; and security measures to be maintained (for NBFCs).
c. Guidelines issued by the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations, 2011: cybersecurity framework for banks based on the Gopalakrishna Committee Report.
d. Cybersecurity Framework in Banks, 2016: instructions to banks on setting up cybersecurity policies and committees, and having security oversight mechanisms in place based on the Gopalakrishna Committee Report.
e. Guidelines on the Sharing of Information Technology Resources by Banks, 2013: guidelines on sharing IT resources to optimise costs while maintaining the desired levels of security measures in place.
f. Information Technology Framework for the NBFC Sector, 2017: IT framework for NBFCs focusing on IT governance; IT policy; information & cybersecurity; IT operations; IS audit; business continuity planning; and IT services outsourcing.

The insurance sector is subject to compliances under the Guidelines on Information and Cyber Security for Insurers issued by the IRDAI, which requires them, *inter alia*, to institute a CISO, formulate a cyber crisis management plan and conduct audits.

Telecommunications Sector
The Unified License, which is required to be entered into by entities providing services in the telecommunication sector for provision of various services, contains specified security measures that need to be followed. These include the following:

a. The licensee will not employ bulk encryption equipment in its network. A licensor or officers specially designated for the purpose may evaluate any encryption equipment connected to the licensee's network.
b. Protection of privacy of communication should be ensured, including any information about a third party and its business to whom it provides the services.
c. The licensee will be responsible for security of their networks.
d. The licensee must have organisational policies on security and security management of their networks, including network forensics, network hardening, network penetration test and other risk assessment measures. Actions to fix these problems and to prevent such problems from recurring should be part of the policy. These policies should be submitted to the Department of Telecommunications and should be audited.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Section 85 of the IT Act imposes liability on companies, wherein, any person who was supervising the affairs of the company at the time any offence was committed, can be made liable. Additionally, Section 85(2) of the IT Act provides that, if a contravention of a rule, direction or order was done with the consent or connivance of a director, manager, secretary or officer of the company, such director, manager, secretary or officer can be made liable. However, no specific offence is provided in respect of Incident reporting. Failure to report may attract liability under the residual penalty provision of the IT Act.

Furthermore, the CMA Rules provide that the Managing Director, or any other director or officer of the company, as the Board may decide, will be responsible for the maintenance and security of electronic records. This will include specific obligations such as:

a. provide adequate protection against unauthorised access, alteration or tampering of records;
b. insure against loss of the records as a result of damage to the storage media;
c. ensure that computer systems, software and hardware are adequately secured and validated to ensure their accuracy, reliability and consistent intended performance;
d. ensure that the records are, at all times, capable of being retrieved to a readable and printable form;
e. ensure periodic backups and limited access;
f. ensure that any reproduction of non-electronic original records in electronic form is complete, authentic, true and legible when retrieved; and
g. take necessary steps to ensure security, integrity and confidentiality of records.

Therefore, failure to implement the above measures, read with general due diligence principles to be followed by directors, may be regarded as a breach of directors' duties.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

These requirements apply to regulated entities such as insurers, banks and telecommunication companies, as well as any organisation having a "protected system". These are not general obligations for all companies.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

As per SEBI circular no. SEBI/HO/IMD/DF2/CIR/P/2019/12, mutual fund and asset management companies are required to submit quarterly reports containing information on cyber-attacks and threats experienced by them, and measures taken to mitigate vulnerabilities, threats and attacks, including information on bugs/vulnerabilities/threats that may be useful for other mutual fund and asset management companies in a soft copy.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

As per SEBI circular no. SEBI/HO/MIRSD/CIR/PB/2018/147, brokers and depository participants are required to formulate a comprehensive cybersecurity and cyber resilience policy document. The policy document is required to be approved by the board or proprietor of the broker and depository participant. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

A civil action for damages can be brought against a "body corporate" under Section 43A of the IT Act, in relation to any Incident, by an affected party.

Section 43A proscribes negligence on the part of a "body corporate", dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, in implementing and maintaining reasonable security practices and procedures.

The elements to be satisfied in order to bring such a civil action for damages under Section 43A of the IT Act are as follows:

i. the body corporate must have acted in a negligent manner in implementing and maintaining reasonable security practices and procedures; and
ii. such negligence must have caused: (a) wrongful loss; or (b) wrongful gain to any person.

Additionally, Section 43A has to be read in conjunction with the SPDI Rules. The SPDI Rules prescribe certain measures/practises that a "body corporate", under Section 43A of the IT Act, must deploy in order to be compliant with the requirement of "implementing and maintaining reasonable security practices and procedures" as prescribed under the IT Act. These measures/practices to be followed by "body corporates", *inter alia*, include the following:

i. the body corporate must adopt and follow a privacy policy;
ii. the body corporate must obtain written consent from the person whose personal information is to be collected, informing him in advance of: (a) the purpose that such information is being collected; (b) the intended receivers of such information; and (c) the name of the agency that will store such data; and
iii. the body corporate must adopt reasonable security measures, including a comprehensive information security policy on managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.

A civil action for damages under Section 43A of the IT Act would have a high likelihood of succeeding if a body corporate is found non-compliant with the measures/practices set out in (i) to (iii) above (among others) and prescribed under the SPDI Rules.

Additionally, a civil action can be brought against any person who commits any acts mentioned in Section 43 of the IT Act without permission of the owner or any other person in charge of a computer, computer system or computer network. Section 43 of the IT Act can be differentiated from Chapter XI of the IT Act, which deals with cybercrime and offences, on the ground that under Chapter XI of the IT Act, the act (*actus reus*) must be accompanied with an intention to commit the act (*mens rea*). The acts defined in Section 43 of the IT Act include, *inter alia*, access to a computer, copying of any data, introduction of or causing introduction of any virus, damaging or causing damage of any program or data within a computer, computer system or network which disrupts its functioning.

A civil action will lie in cases where such acts are committed without any intention. The penalty prescribed for any person who is held liable are damages by way of compensation to the person affected by such acts.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Following is an illustrative list of cases that have been instituted before Courts/adjudicatory forums in India in relation to Incidents:

Hacking

In *State Bank of India v. Chander Kalani & Ors.*, Cyber Appeal No. 13 of 2015 (M.A. No. 282 of 2017), the Telecom Disputes Settlement and Appellant Tribunal ("**TDSAT**"), New Delhi was adjudicating a dispute pertaining to alleged hacking of the complainant's email ID and leak of confidential information pertaining to the complainant's bank account. The complainant alleged that the bank, i.e. State Bank of India ("**SBI**"), was negligent in disclosing details of the complainant's bank account by responding to fake emails and was, therefore, liable to pay the complainant compensation under Section 43A of the IT Act.

The TDSAT held that "*on a careful reading of Section 43A, it is absolutely clear that negligence in implementing and maintaining reasonable security practices and procedures alone creates a liability to pay damages or compensation under Section 43A, if such negligence has caused wrongful loss or wrongful gain to the person affected […] For this Section to apply, firstly, the body corporate should be possessing, dealing or handling sensitive personal data or information in a computer resource under its ownership, control or operation. Secondly, it should be found negligent in implementing and maintaining reasonable security practices and procedures and thirdly, by such negligence it caused wrongful loss or wrongful gain to any person*".

Phishing

In *Umashankar Sivasubramanian v. ICICI Bank*, Petition No. 2462 of 2008, the Adjudicating Officer under the IT Act at Chennai was deciding a dispute pertaining to phishing. In this case, the complainant received a fake security update email and, assuming that it was from ICICI Bank, shared certain details of his bank account. Pursuant to sharing this information, a certain amount was debited from the complainant's account. The Adjudicating Officer held that

the ICICI Bank failed to exercise due diligence by not preventing "unauthorised access", as contemplated under Section 43 of the IT Act.

On appeal, the TDSAT held "*the appellant is correct in submitting that Section 43A has been inserted in the Act at a later date and therefore, appellant cannot be held liable for paying damages by way of compensation only for failure to protect any sensitive personal data or information available in appellant's computer resource*". The relevant provision to this case was Section 43(g).

The Tribunal recognised the imbalance of power between the Bank and its customers, and held that "*Terms and conditions governing Internet Banking appearing on the website of the Bank in fine prints cannot absolve the Bank from its liability of providing adequate security measures so that requirements of the Act, the rules and regulations made thereunder are met satisfactorily and the customers' interests are well protected*".

Even though Section 43A was not applicable, the Tribunal held that the existing definition of the word "computer" in the Act is wide enough to include all input, output processing and storage. The Tribunal held that "*The Bank has failed to show by way of defense that it had taken all the required precaution and that the SMTP Server which it was using in 2007 was the most technically advanced Server then available but even then the Bank failed to secure its Email system against misuse. Hence, we find no good reasons to reverse or in any way interfere with the finding and order of the Adjudicating Officer in so far as compensating the respondent for the loss of his money*".

In *National Association of Software and Service Companies v. Ajay Sood and Ors.*, 119 (2005) DLT 596, the Delhi High Court decreed a settlement between the plaintiffs and defendants in a case pertaining to phishing, wherein the defendants were masquerading as the plaintiff and sending fraudulent emails, using the plaintiff's trademark "NASSCOM", with a view of obtaining personal data of various addresses.

The court recognised phishing as a form of internet fraud, where a person pretending to be a legitimate association such as a bank or an insurance company extracts personal data from a user, such as access codes and passwords, which are then used to his own advantage. This case brought phishing into the ambit of Indian law even in the absence of specific legislation.

Cybersquatting

In *Raymond Limited v. Raymond Pharmaceutical Pvt. Ltd.*, 2017 (69) PTC 79 (Bom), the Bombay High Court was adjudicating a notice of motion filed by the plaintiff seeking an injunction against the defendant from using the mark "raymond" as part of their domain name www.raymondpharma.com. In this case the Court distinguished "cybersquatting" from trademark infringement and ruled that the defendant was guilty of neither by using the mark "raymond" as part of their domain name.

Infringement action in respect of trademarks is largely based on the need to protect a consumer of products or services to ensure that the consumer or purchaser receives goods or services that they think that they are paying for. On the other hand, cybersquatting is typically characterised by the defendant attempting to sell a domain name corresponding with that of the plaintiff, with the intent to sell it to the plaintiff or the plaintiff's competitor. The Court opined that the required elements of "cybersquatting" were not satisfied by the defendant in the present case.

Breach of confidentiality

In *Olive e-business v. Kirti Dhanawat & Ors.*, the Delhi High Court passed an ex-parte interim injunction restraining the defendants from misusing and misappropriating trade secrets and confidential information of the plaintiff without authorisation. As part of this injunction, the Court also ordered Google (arrayed as a defendant to the suit) to block the email accounts of the other defendants in the suit.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Incidents which amount to civil wrongs may attract tortious liability. The IT Act broadly identifies Incidents from which potential plaintiffs may recover. However, the IT Act's enumeration of cyber-attacks may not always offer the most adequate remedies. Often, reimagining cyber-attacks as traditional torts make for better claims. For example, a denial-of-service attack may amount to nuisance, introduction of ransomware, trojans and/or viruses may amount to conversion by destruction, hacking may be treated as trespassing and phishing may amount to fraudulent misrepresentation.

Hacking may be treated as trespassing on virtual property considering the quantity and worth of data that can be stored on computer systems. Trespass actions can no longer be stranded in the idea of protecting an owner's control over their *physical* property. Similar to trespass, when a computer system is hacked without any criminal intent, the hacking is of a civil nature. When the intention to cause harm accompanies the act of hacking, there is criminal liability. For instance, a denial of service attack prevents intended users of the machine or network from accessing it, disrupting the normal course of business and creating a nuisance. If the discomfort or inconvenience caused is considered material and substantial, then a case can be made for liability under tort law.

Pertinently, data breaches could snowball into other torts. Banks and financial institutions are reportedly under relentless cyber-attacks, (please see https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security; and http://www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf.aspx?ext=) and going forward need to invest more resources into cybersecurity infrastructure. Attacks targeted at institutions like banks, law firms and stock exchanges could expose sensitive information, the publication of which has the possibility of causing loss, such as due to dramatic fall in share value. In theory, plaintiffs could bring an action in tort to make good these losses. Equally, actions based in breach of privacy or confidence, recklessness, or negligence are a possibility at a time where online banking is being used more than ever, even to deliver government based benefits to the masses (please see https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms).

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

There is no express prohibition against taking out insurance in this regard. Cybersecurity insurances are commonly offered in India. However, statutory liability will not be mitigated through such insurance.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There is no such regulatory limitation.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Maintaining access protocols in respect of electronic records is a statutory requirement in certain cases such as when a company is part of a regulated sector or has a "protected system". Furthermore, employee monitoring may be part of the internal information security policy of a particular company. It is not a general requirement in law. In addition, there is no statutory requirement on employees to generally report cybersecurity Incidents to the management and this is also typically governed by internal policies.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There is no such concern.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The IT Act provides for the following general powers for law enforcement:

a. **Confiscation** – Any computer resources in respect of which any contravention of the IT Act has been carried out, can be confiscated.
b. **Issuing directions for decryption/monitoring of resources** – If necessary, for national security and allied purposes, authorised government officers can issue orders to intercept, monitor or decrypt any computer resource.
c. **Blocking orders** – If necessary, for national security and allied purposes, intermediaries providing access to any information may be required to block access to any information stored, received or generated in any computer resources.
d. **Monitor/collect traffic data** – Law enforcement agencies can be authorised to monitor and collect traffic data or information generated, received or transmitted in any computer resource.

Offences under the IT Act are to be investigated by a police officer not below the rank of Inspector.

Please note that there are exceptions provided in specific laws for compliance with law enforcement access requests. An illustrative list is provided below:

a. The SPDI Rules require consent to be sought from the provider of sensitive personal information before disclosure of the same to any third party – however, law enforcement agencies requiring such information for the purpose of investigation are an exception to this.
b. For intermediaries under law, such as search engines and social media websites that are exempted from liability with respect to content on their platform because they act as neutral conduits of information, one of the preconditions for retaining safe harbour is compliance with law enforcement access requests for information and takedown of content.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

As specified in question 8.1, the IT Act provides law enforcement authorities with the power to monitor and intercept any computer resource. Furthermore, under the provisions of the IT Act, read in conjunction with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**IMD Rules**"), an intermediary under law is obligated to provide co-operation and assistance in respect of monitoring and decryption orders. If a decryption order under the IMD Rules is issued to the decryption key holder, the latter will provide time bound assistance in decryption of resources, including disclosure of decryption key.

Acknowledgments

The authors would like to acknowledge the assistance of Richa Srivastava, Raktima Roy and Abhishek Jain.

GV Anand Bhushan is the Head for Chennai Office and Partner at the Firm since July 1, 2016. He was awarded Technology Lawyer of the Year by the Indian National Bar Association in 2017 in recognition of his work in the field. Prior to that, he was a Board Member and General Counsel, APAC at Cognizant Technology Solutions and negotiated deals that generated revenue worth several billion dollars across IT services and other emerging technologies. He was honoured as the General Counsel of the Year 2014, as an innovation champion for introducing innovative leadership and processes at Cognizant.

Shardul Amarchand Mangaldas & Co.
Express Towers, 23rd Floor
Nariman Point
Mumbai 400 021
India

Tel: +91 22 4933 5555
Email: gvanand.bhushan@amsshardul.com
URL: www.amsshardul.com

Tejas Karia is a Partner at Shardul Amarchand Mangaldas & Co. He specialises in Information Technology Law and International Arbitration. He regularly advises multinational and Indian corporations on data protection, data security, data retention, privacy and confidentiality issues, including data belonging to third parties and employees. He represents prominent social networking websites and internet messaging services in numerous litigations in India.
He has advised the National Association of Software and Service Companies ("**NASSCOM**") for amendments to the Indian Information Technology Act, 2000 to include the Data Protection provisions. He is a member of the Editorial Board of "Digital Evidence and Electronic Signatures Law Review", a quarterly journal published in UK. He is also co-author of the chapter on India in the book "Digital Evidence".
He has been recognised as a "Leading Lawyer" by *Asialaw* Leading Lawyers, mentioned in *The Legal 500*, ranked by *Chambers & Partners*, listed in *Who's Who Legal* and named as "Dispute Resolution Star" by *Benchmark Litigation*.

Shardul Amarchand Mangaldas & Co.
Amarchand Towers
216 Okhla Industrial Estate, Phase III
New Delhi 110 020
India

Tel: +91 11 4159 0700
Email: tejas.karia@amsshardul.com
URL: www.amsshardul.com

Shahana Chatterji is a Partner in the Public Policy and Regulatory Affairs team at Shardul Amarchand Mangaldas. Shahana works closely with the world's largest technology, internet and social media companies on matters relating to data privacy, cybersecurity and risk profiling for disruptive technologies, including AI solutions in the healthcare sector, e-commerce, cloud computing, public procurement of technology, payment technology and fintech solutions.
Recently, she has led critical matters for her clients and thought leadership for the industry on the proposed data protection framework in India, which resulted from the Srikrishna Expert Committee and the nation-wide consultations it held. Key data protection projects she has advised on include workplace privacy, employee investigations, GPS data and location sharing, biometric data collection and authentication, targeted advertising and marketing, cloud computing and cross-border data transfers. She has also advised clients on cybersecurity issues including secure management of data assets and Incident reporting.

Shardul Amarchand Mangaldas & Co.
Express Towers, 23rd Floor
Nariman Point
Mumbai 400 021
India

Tel: +91 22 4933 5555
Email: shahana.chatterji@amsshardul.com
URL: www.amsshardul.com

Ireland

Maples Group

Kevin Harnett

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

The Criminal Justice (Offences Relating to Information Systems) Act 2017 (the "2017 Act") came into force on 12 June 2017, giving effect to Directive 2013/40/EU regarding criminal attacks against information systems.

Hacking (i.e. unauthorised access)
Hacking is an offence in Ireland, which, under section 2 of the 2017 Act, occurs when a person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure.

Denial-of-service attacks
Denial-of-service attacks constitute an offence under the 2017 Act, captured under section 3, which provides that it is an offence when a person who, without lawful authority: intentionally hinders or interrupts the functioning of an information system by inputting data on the system; transmits, damages, deletes, alters or suppresses, or causes the deterioration of, data on the system; or renders data on the system inaccessible.

Phishing
Phishing does not, *per se*, constitute a specific offence in Ireland. However, it is possible that the activity would be caught by certain other, more general criminal legislation, depending on the circumstances (for instance, relating to identity theft or identity fraud). In this regard, see below.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware is also an offence, again covered by the 2017 Act. In this regard, section 4 provides that a person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of data on an information system commits an offence.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Possession or use of hardware, software or other tools used to commit cybercrime also constitutes an offence under the 2017 Act (section 6), which occurs when a person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under the 2017 Act, certain hacking tools. Such tools are described as "(i) any computer programme that is primarily designed or adapted for use in connection with the commission of such an offence, or (ii) any device, computer password, unencryption key or code, or access code, or similar data, by which an information system is capable of being accessed".

Identity theft or identity fraud (e.g. in connection with access devices)
Although there is no precise, standalone offence of identity theft or identity fraud in this jurisdiction, it can nonetheless potentially be captured by the more general offence referred to as "making a gain or causing a loss by deception" (as contained in section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (the "2001 Act")). This occurs where a person who dishonestly, with the intention of making a gain for himself or herself or another, or of causing loss to another, by any deception induces another to do or refrain from doing an act. In addition, sections 25, 26 and 27 of the 2001 Act cover specific forgery offences.

Separately, under section 8 of the 2017 Act, identity theft or fraud is an aggravating factor when it comes to sentencing, in relation to "denial-of-service attack" or "infection of IT systems" offences. This is described in broad terms as being a misuse of the personal data of another person with the aim of gaining the trust of a third party, thereby causing prejudice to that person.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is covered by the relatively broad offence of "unlawful use of a computer", as provided for in section 9 of the 2001 Act. This occurs where a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Section 5 of the 2017 Act creates the offence of "intercepting the transmission of data without lawful authority", which occurs when a person who, without lawful authority, intentionally intercepts any transmission (other than a public transmission) of data to, from or within an information system (including any electromagnetic emission from such an information system carrying such data). This is a broad provision which potentially covers other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

With regard to penalties, in relation to offences under the 2017 Act, the penalties range from maximum imprisonment of one year and a maximum fine of €5,000 for charges brought "summarily" (i.e., for less serious offences), to a maximum of five years' imprisonment (10 years in the case of denial-of-service attacks) and an unlimited fine for more serious offences. The above offences under the 2001 Act are only tried in the Circuit Court, with "making a gain or causing a loss by deception" carrying a maximum penalty of five years' imprisonment and an unlimited fine, and forgery and "unlawful use of a computer" offences carrying a maximum of 10 years and an unlimited fine.

Owing to the relatively recent implementation of the 2017 Act, there have been very few (if any) prosecutions of note under this particular legislation to date. That said, Ireland's first successful prosecution for hacking took place in July 2013 on foot of charges under the Criminal Damage Act 1991. The prosecution followed a collaborative investigation between the Irish Garda Bureau of Fraud and the FBI, and involved the hacking of a major political party's website during the run-up to a national election.

There have also been a number of relatively high-profile denial-of-service attacks on large national websites over the last couple of years (those of certain governmental departments and the national lottery, to name a few), which are currently the subject of ongoing investigations. These investigations may lead to some element of prosecution under the 2017 Act in the near future.

Failure by an organisation to implement cybersecurity measures

There is no particular offence in this jurisdiction directly linked to a failure by an organisation to implement cybersecurity measures. That said, and in specific relation to personal data concerning individuals, section 71 of the Data Protection Act 2018 (the "**DPA**") provides that controllers must ensure that data is "processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against (a) unauthorised access or unlawful processing, and (b) accidental loss, destruction or damage".

The Data Protection Commission (the "**DPC**") may, under its statutory powers, notify an organisation that it is deemed to have breached these obligations, and further issue an enforcement notice in this respect. It is then an offence for any controller or processor to, without reasonable excuse, fail or refuse to comply with such a notice. The maximum fine imposable in this regard is €250,000 or imprisonment for a term not exceeding five years.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above offences under the 2017 Act have certain extraterritorial application, and so offenders may therefore be tried in Ireland, so long as they have not already been convicted or acquitted abroad in respect of the same act, and the relevant act was committed:

(a) by the person in Ireland in relation to an information system outside of the country;
(b) by the person outside of the country in relation to an information system in Ireland; or
(c) by the person outside of the country in relation to an information system also outside of the country, if:
    (i) that person is an Irish citizen, a person ordinarily resident in Ireland, or a company established or existing under Irish law; and
    (ii) the act is an offence under the law of the place where it was committed.

Although broader concepts such as, for instance, the "European arrest warrant" may be of relevance for Irish prosecutors, none of the above-mentioned offences under the 2001 Act carry, in and of themselves, extraterritorial application.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Each of the above offences under the 2017 Act contain the ingredient that it was committed without "lawful authority", which is defined as either "with the authority of the owner of the system", "with the authority of a right holder of the system", or "as permitted by law". Accordingly, prosecution of these offences will require, necessarily, that such authority or lawful permission was absent.

In addition, the offence relating to "hacking" carries a further qualification, i.e., where the person or company had a "reasonable excuse". This term is, however, not defined under the 2017 Act, and so its precise application will depend on future judicial interpretation.

In addition, if a company is charged with any of the above 2017 Act offences where the offence was committed by an employee for the benefit of that company, it will be a defence for that company that it took "all reasonable steps and exercised all due diligence" to avoid the offence taking place.

Separately, it can be expected that judges will continue to take established factors into account when considering the appropriate penalty on foot of a conviction of a cybersecurity-related crime (e.g., remorse, amends, cooperation with investigators, criminal history, and extent of damage).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

It is, for instance, an offence under section 8 of the Offences against the State (Amendment) Act 1998 to "collect, record or possess information which is of such a nature that it is likely to be useful in the commission by members of any unlawful organisation of serious offences generally or any particular kind of serious offence". The term "serious offence" would encompass any of the above-mentioned offences (apart from failure to comply with an enforcement notice issued by the DPC), so long as the act in question is one which involves "serious loss of or damage to property or a serious risk of any such loss…or damage". The maximum sentence for this offence includes an unlimited fine and 10 years' imprisonment. To date, there does not appear to have been any prosecutions of note which have combined this particular offence with acts of cybercrime.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Apart from the above-referenced statutes in respect of criminal activity, Applicable Laws include the following:

- Data Protection: The DPA governs the manner in which personal data is collected and processed in Ireland. The DPA

requires that controllers take "appropriate security measures" against unauthorised access, alteration, disclosure or destruction of data, in particular where the processing involves transmission of data over a network. The DPA adopted the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") to Irish law in May 2018.

- e-Privacy: The e-Privacy Regulations 2011 (S.I. 336 of 2011), which implemented the e-Privacy Directive 2002/58/EC (as amended by Directives 2006/24/EC and 2009/136/EC) (the "**e-Privacy Regulations**"), regulate the manner in which providers of publicly available telecommunications networks or services handle personal data and require providers to take appropriate technical and organisational measures to safeguard the security of its services and report Incidents. It was intended that a revised EU e-Privacy Regulation be introduced in May 2018 to replace the existing e-Privacy Directive and e-Privacy Regulations, expanding the current regime to cover all businesses which provide online communication services. That new regulation is still in draft form and at the date of writing has not yet been finalised.
- Payments Services: The new Payments Services Directive II (Directive 2015/2366/EU), was transposed by the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) (the "**Payment Services Regulations**") on 12 January 2018, and introduced regulatory technical standards (which were published by the European Banking Authority) to ensure "strong customer authentication" and payment service providers will be required to inform the national competent authority in the case of major operational or security Incidents. Providers must also notify customers if any Incident impacts the financial interests of its payment service users. The Payment Services Regulations superseded the previous regime which was introduced in 2009.
- The Security of Network and Information Systems Directive 2016/1148/EU (the "**NISD**") was transposed into Irish law in September 2018 under S.I. 360/2018 and is known as the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 ("**NISD Regulations**"). The NISD seeks to harmonise cybersecurity capabilities and achieve a common level of network and information systems security across the EU by increasing cooperation amongst EU Member States, improving national capabilities and introducing security measures and Incident reporting obligations for certain operators of essential services.
- Other: If there is a security breach which results in the dissemination of inaccurate information, persons about whom the inaccurate data relates may seek a remedy under the Defamation Act 2009. Similarly, if information was provided in confidence and such information was leaked, there may be an action under common law for breach of confidence or negligence, in the event that a duty of care is found to have been owed.

See also sections 1 and 5.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

As noted above, the NISD was transposed into Irish law in September 2018 under the NISD Regulations. The NISD is also the subject of Commission Implementing Regulation (EU) 2018/151, which specifies further elements to be taken into account when identifying measures to ensure security of network and information systems. Publicly available telecommunications networks and services are governed by the e-Privacy Regulations outlined at question 2.1 above.

We do not believe that the implementing legislation exceeds the requirements of the NISD in any material way.

The Department of Communications, Climate Action and Environment ("**DCCAE**")) published the National Cyber Security Strategy 2015–2017, which provides a mandate for the National Cyber Security Centre to engage in activities to protect critical information infrastructure. In March 2019 the Government opened a public consultation designed to consider what a new, replacement strategy should focus on. That public consultation has now closed and a new National Cyber Security Strategy is expected shortly. As matters stand, the DCCAE together with the Government Taskforce on Emergency Planning and the Office of Emergency Planning in the Department of Defence operate as lead government departments for emergency situations relating to, inter alia, critical infrastructure.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the DPA, controllers are required to take appropriate measures, as outlined in questions 1.1 and 2.1 above. The DPA does not detail specific security measures to be undertaken but in determining appropriate measures, a controller may have regard to the state of technological development and the cost of implementing the measures. Controllers must ensure that the measures provide a level of security appropriate to the harm that might result from a breach and the nature of the data concerned. The DPC has issued guidance which suggests the introduction of measures such as access controls, automatic screen-savers, encryption, anti-virus software, firewalls, software patching, secure remote access, back-up systems and Incident response plans.

Under the e-Privacy Regulations, providers of publicly available telecommunications networks or services are required to take appropriate technical and organisational measures and ensure the level of security appropriate to the risk presented, having regard to the state of the art and cost of implementation. Such measures shall at least ensure that personal data can only be accessed by authorised personnel for legally authorised purposes, protect personal data against accidental or unlawful destruction, loss, alteration, processing, etc., and ensure the implementation of a security policy.

The NISD Regulations require that operators of essential services take appropriate measures to prevent and minimise the impact of Incidents affecting the security of the network and information systems used for the provision of essential services with a view to ensuring continuity. Similarly, digital service providers are required to identify and take appropriate and proportionate technical and organisational measures to manage risks posed having regard to the state of the art and take account of, *inter alia*, the security of the systems and facilities, Incident handling, business continuity management and compliance with international standards.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Applicable Laws are largely harmonised at an EU level, and as such the risk of conflicts of laws is minimised. However, the existence of differing requirements for organisations with operations both within the EU and externally may present compliance challenges for such companies.

With regard to the confidentiality of electronic communications, it is understood that updated interception legislation is in the process of being prepared, namely the Interception of Postal Packets and Telecommunications Messages (Regulation) (Amendment) Bill. This was included in the Government's autumn 2019 legislative programme, but has not been prioritised for the current legislative session. The purpose of the bill is to update the Postal and Telecommunications Acts 1983 and 1993, which are limited in scope to postal services and traditional telecommunications providers, to regulate the lawful interception of all communications delivered over the internet.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Section 86 of the DPA contains a general personal data breach notification obligation to the DPC. Where a personal data breach occurs, the controller shall without undue delay and, where feasible, within 72 hours of becoming aware of the breach, notify the DPC of the breach. This notification shall include a description of the breach, the number or approximate number of data subjects concerned and personal data records concerned. It must also contain a list of likely consequences of the breach and measures taken or proposed to be taken to address the breach.

Where a data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject, Section 87 of the DPA requires the controller to notify the data subject to whom the breach relates. The requirement is waived where the controller has implemented appropriate measures to protect the data; in particular where the measures render the data unintelligible through encryption or otherwise to any person not authorised to access it. This notification must contain at least the same information provided to the DPC as described above.

Providers of publicly available telecommunications networks or services are required to report information relating to Incidents or potential Incidents to the DPC (to the extent that such Incidents relate to personal data breaches). In the case of a particular risk of a breach to the security of a network, providers of publicly available telecommunications networks or services are required to inform their subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved. In case of a personal data breach, such providers must notify the DPC without delay and where the said breach is likely to affect the personal data of a subscriber or individual, notify them also. If the provider can satisfy the DPC that the data would have been unintelligible to unauthorised persons, there may be no requirement to notify the individual or subscriber of the breach.

Under Article 17of the NISD Regulations, operators of essential services must notify the National Cyber Security Centre without delay of any Incident having a substantial impact on the provision of a service. The notification must provide sufficient information so that the National Security Cyber Centre can assess the significance of same and any cross-border impact. The NISD Regulations stipulate that notification shall not make the notifying party subject to increased liability.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

See above at question 2.5 regarding the requirement to notify the DPC.

The National Cyber Security Strategy published in 2015 outlines the intention of the DCCAE to deepen its partnerships with third-level institutions to aid the sharing of knowledge, experience and best practice. Moreover, the Strategy outlines the active information-sharing role between the DCCAE and other public sector bodies and industry at the time (including IRISS-CERT). Under the NISD Regulations, the CSIRTs Network is tasked with exchanging and making available, on a voluntary basis, non-confidential information concerning individual Incidents.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See question 2.5 above.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Parties must ensure that personal data is processed (e.g., shared) in accordance with the DPA and take appropriate security measures with regard to any onward transmission of data including in the context of notifications of Incidents. Personal data includes data relating to a living individual who is or can be identified from either the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the controller. There are exemptions under the DPA such as for the processing of data which is necessary for the administration of justice or to enable the

controller to comply with a legal obligation. Therefore, different considerations apply in the context of voluntary sharing of personal data relating to a breach, and mandatory reporting. For that reason, controllers should take particular care when a notification includes any personal data and take steps to anonymise data where appropriate. Additional considerations also apply in the case of 'special categories of personal data' as set out in Part 3, Chapter 2 of the DPA.

Parties must also be conscious of their contractual obligations and whether issues may arise regarding the sharing of price-sensitive or confidential information, particularly if there is no mandatory requirement to do so.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The DPC is the primary regulator responsible for enforcing the requirements outlined above. The DPC is an independent body established under the DPA.

Under the NISD, the national competent authority is the National Cyber Security Centre.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There is no automatic penalty for controllers under the DPA in the event of a data breach. However, if the DPC issues an information notice (requiring certain information) or enforcement notice (requiring certain action), a controller or processor must comply with same. If they do not comply, it will constitute an offence. The DPC (unlike under the previous regime) can now impose administrative fines directly as follows:

- a maximum of €5,000 or imprisonment for a term not exceeding 12 months or both on summary conviction; and
- a maximum of €250,000 or imprisonment for a term not exceeding five years or both for conviction on indictment.

The original draft of the DPA exempted public bodies from administrative fines, but following intense lobbying, the DPA now provides for fines of up to €1 million in respect of those bodies.

Further, the DPA also incorporates in Section 141 the right of the DPC, as the supervising authority, to impose fines of up to €20 million or 4% of global turnover as set out in Article 83 of the GDPR.

Under the e-Privacy Regulations, a person who commits an offence is liable on summary conviction to a fine. Furthermore, if a person is convicted of an offence, the court may order any material or data that appears to it to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In the first half of 2018 the DPC completed its investigation into Yahoo! EMEA Limited ("**Yahoo!**") following a data breach at that company which was first reported in 2016, where material was taken from approximately 500 million user accounts.

The investigation concluded amongst other things that Yahoo!'s security policies did not take adequate account of its obligations under data protection laws. It was instructed by the DPC to review and update its policies to so take account of data protection laws.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of beacons for such purposes.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of honeypots for such purposes.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of sinkholes for such purposes.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, market practice with respect to information security varies considerably in Ireland dependent on the industry sector concerned. Businesses in industries that are recognised as being particularly vulnerable to Incidents, such as the financial services sector, are more likely to have adequate processes in place to effectively address cyber risk. With current and long-term trends, such as the continued expansion of cloud computing, mobile data and the internet of things further increasing exposure to cyber risk, financial services firms are expected to update and implement their processes accordingly. The publication of the Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks by the regulator for financial institutions, the Central Bank of Ireland, provides valuable information on the practices that financial services firms are expected to apply in order to protect their organisations from cyber threats.

Other industries have previously been less cognisant of the need for adequate cybersecurity protections. For example, the manufacturing industry in Ireland has been largely unaffected by Incidents. However, advances in robotics, technology and the digital marketplace have increased the awareness of manufacturers to the need for maintenance and protection of cyber infrastructure. In response to this, IBEC, the largest business and employer association for organ-

isations based in Ireland, has highlighted the prioritisation of cybersecurity as a key component in the development of the manufacturing industry in Ireland and has set out a number of recommendations in a recent report setting out their short- to medium-term strategy for Ireland's manufacturing industry.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) There is currently no specific legislation focused on cybersecurity applicable to organisations in the financial services sector. In the absence of any codified law, the Central Bank of Ireland has published Cross Industry Guidance, which relates to IT governance and risk management by regulated financial institutions in Ireland. The publication makes a number of recommendations including (but not limited to): the preparation of a well-considered and documented strategy to address cyber risk; the implementation of security awareness training programmes; the performance of cyber risk assessments on a regular basis; and the implementation of strong controls by firms over access to their IT systems. The NISD Regulations introduce security measures and Incident reporting obligations for credit institutions. See also reference to Payment Sources Regulations in question 2.1 above.

(b) While there are no specific laws on cybersecurity, electronic communications companies (such as telecoms companies and ISPs) are governed by the DPA, and also the e-Privacy Regulations. Under the e-Privacy Regulations, there are more explicit rules governing the security of personal data. The electronic communications sector has been further affected by the introduction of the DPA in May 2018. Businesses in the sector have had to familiarise themselves with the new requirements introduced, notably in the areas of transparency, security and accountability for controllers and processors. Certain operators (IXPs, DNS service providers and TLD name registries) also now fall within the ambit of the NISD Regulations.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

While there are no express directors' duties specific to cybersecurity, directors owe fiduciary duties to their company under common law and under the Companies Act 2014 (the "**CA 2014**").

There are a number of key fiduciary duties of directors set out in the CA 2014. This list, however, is not exhaustive. Some examples of directors' duties which could be considered to extend to cybersecurity are:

- exercise their powers in good faith in what the director considers to be the interests of the company;
- act honestly and responsibly in relation to the conduct of the affairs of the company;
- act in accordance with the company's constitution and exercise his or her powers only for the purposes allowed by law;
- exercise the care, skill and diligence which would be exercised in the same circumstances by a reasonable person having both the knowledge and experience that may reasonably be expected of a person in the same position as the director with the knowledge and experience which the director has; and
- have regard to the interests of its employees in general.

Directors have a general duty to identify, manage and mitigate risk, as well as fiduciary duties, such as those outlined above, which would extend to cybersecurity. Such duties could be interpreted to mean that directors should have appropriate policies and strategies in place with respect to cyber risk and security and that directors should review and monitor these on a regular basis. Regard may also be had to compliance by a company with all relevant legislative obligations imposed on that company in assessing compliance by directors with their duties. Appropriate insurance coverage should also be considered.

Directors should be fully briefed and aware of all of the key issues relating to cyber risk. Larger organisations may choose to delegate more specific cyber risk issues to a specific risk sub-committee.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

While there are no such express obligations from a company law perspective, general director fiduciary duties, best corporate governance practices, as well as the "appropriate security" requirements under the DPA, may dictate that such actions are performed. See question 4.1 above for more detail on directors' duties. For industry-specific requirements, see question 3.1 above.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

While there are no such express obligations from a company law perspective, general director fiduciary duties, as well as best corporate governance practices, may dictate that such actions are performed. See question 4.1 above for more detail on directors' duties.

The e-Privacy Regulations oblige electronic communications service providers to report all data breaches to the DPC. The DPA has introduced a more general personal data breach notification obligation to the DPC, which may be of relevance to an Incident. The NISD Regulations introduced Incident reporting obligations for certain operators of essential services. Where an Incident is relevant to the carrying out of a function regulated by the Central Bank of Ireland, this may give rise to a disclosure requirement to the Bank.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

This chapter sets out the principal laws and requirements relating to cybersecurity in Ireland. However, there may be other requirements and/or recommendations established by industry-specific codes of conduct. In addition, there may be other laws that do not directly relate to cybersecurity but which establish requirements that bear on cybersecurity. See, in addition, section 2 above.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

As discussed in response to question 5.3 below, an Incident may give rise to various claims under the law of tort. It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract.

In order to be entitled to compensation in damages, whether under a tortious or contractual analysis, a plaintiff will be required to establish: that a duty or obligation was owed to him/her by the defendant; that an Incident has occurred as a result of the defendant acting in breach of that duty or obligation; and loss or damage has been sustained to the plaintiff which would not have been sustained, but for the defendant's conduct.

It should be noted that many classes of Incident will also give rise to claims for damages for breach of the constitutional right to privacy. Moreover, where an Incident is committed by a State actor, for example, during the course of an investigation, it may give rise to an action in judicial review to prevent misuse of any inappropriately obtained data and/or to quash any decision taken in relation to, and/or on foot of, the Incident or any improperly obtained data.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Duggan v Commissioner of an Garda Síochána, Ireland and the Attorney General [2017] IEHC 565 – This case affirmed the previously stated position from *Collins v FBD Insurance Plc* [2013] IEHC 137 that a breach of the Data Protection Acts 1988 and 2003 would not automatically entitle a data subject to compensation irrespective of whether or not they could prove actual loss or damage. The High Court concluded that a data subject has no entitlement to automatic compensation for a technical breach of his/her rights under the Data Protection Acts 1988 and 2003 where he/she cannot prove that he/she has suffered loss or damage as a result of the breach. Under the new regime, Article 82 of the GDPR provides that a person who has suffered material or *non-material* damage as a result of an infringement of the GDPR has a right to compensation. The introduction of a right of action for "non-material" damage will likely result in a lower threshold for recoverability as a result of Incidents with a personal data dimension.

CRH plc and Others v Competition and Consumer Protection Commission [2017] IECS 34 – The Supreme Court upheld the finding of the High Court that, in seizing material unrelated to an investigation, the Competition and Consumer Protection Commission had acted outside the scope of its statutory powers and would be acting in breach of the applicants' rights to privacy were it to examine such material. In the exercise by the State of its powers of search, the Supreme Court held that interference with the right to privacy was inevitable but that such interference must be proportionate.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Depending on the specific type of Incident concerned, liability in tort may arise. Examples of such tortious liabilities are as follows:

- The DPA permits a data subject to take a data protection action against a controller or processor where they believe their rights have been infringed. This is deemed to be an action founded in tort. Importantly, the DPA confirms that the damage for which the data subject is seeking compensation need not be just financial. A data subject can sue for other types of damage including pain and suffering.
- A breach of a person's privacy rights may give rise to a claim in tort for breach of confidence or negligence, depending upon the circumstances.
- Incidents involving the theft of information or property may give rise to claims in the tort of conversion.
- Incidents involving the publication of intrusive personal information may in some circumstances constitute the tort of injurious or malicious falsehood.
- Incidents involving the misuse of private commercial information may give rise to claims for damages for tortious interference with economic relations.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

"Cyber insurance" products are being taken up by businesses with increasing frequency and are now seen as routine. Such products afford cover for various data- and privacy-related issues including: the financial consequences of losing or mis-appropriating customer or employee data; the management of a data breach and attendant consequences, including the costs associated with involvement in an investigation by the DPC and fines levied for breaches; and the costs associated with restoring, recollecting or recreating data after an Incident.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no legal limits placed on what the insurance policy can cover. In the ordinary way, however, the consequences of intentional wrongdoing tend to be contractually excluded, as are the consequences of failure to remedy ascertained weaknesses or shortcomings in systems.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

An employer should avoid covert and excessive monitoring of employees. Under the DPA and the ECHR, employees are entitled to privacy, which generally means that employers must balance their need to monitor employees for the purposes of protecting their business against the individual employee's right to privacy. Each case would be decided on its particular circumstances.

The Irish whistleblowing legislation, the Protected Disclosures Act 2014, protects employees from penalisation arising out of reporting actual or possible wrongdoing. In addition, the employer should keep in mind its obligations under data protection legislation when processing personal data, including that such data is kept secure and, where applicable, obligations arising under the e-Privacy Regulations and under the NISD. Employees should be made aware, typically by means of a written company policy or relevant provision in the employment contract, of such obligations and their duty to adhere to such obligations on behalf of the company.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No. Whistleblowing laws do not limit or prohibit such reporting by an employee; instead, they are intended to protect the employee from penalisation following his/her making such a report to the employer.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Under the 2017 Act, the Irish police force (generally operating out of the Garda National Economic Crime Bureau) is given a relatively broad authority to investigate cybersecurity Incidents or suspected activity. Specifically, a warrant is obtainable so as to enter and search a premises, and examine and seize (demanding passwords, if necessary) anything believed to be evidence relating to an offence, or potential offence, under the 2017 Act, from a District Court Judge on foot of a suitable Garda statement, on oath.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements under Irish law for organisations to implement backdoors to their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys.

Kevin Harnett joined Maples Group in 2009 and was elected as a partner in 2016. He previously worked for a multinational software company as corporate counsel and prior to that, he trained and practised with a large Irish corporate law firm. Kevin has extensive experience advising both domestic and multinational clients on large and complex commercial disputes, including proceedings before the Commercial Court, as well as all forms of alternative dispute resolution and related advisory work. He has a particular focus on the financial services, technology and construction sectors.

Maples Group
75 St. Stephen's Green
Dublin 2, D02 PR50
Ireland

Tel: +353 1 619 2036
Email: kevin.harnett@maples.com
URL: www.maples.com

Israel

Pearl Cohen Zedek Latzer Baratz

Haim Ravia

Dotan Hammer

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Section 4 of the Israeli Computers Law, 5755-1995 criminalises unlawful intrusion into computer material. The term "intrusion into computerized material" is defined in the statute as "intrusion by communicating with or connecting to a computer, or by operating it, but excluding intrusion that constitutes wiretapping" under the Israeli Wiretap Law, 5739-1979. This offence carries a maximum penalty of three years' imprisonment.

Section 5 of the Computers Law penalises intrusion into computer material committed in furtherance of another predicate felony. The maximum penalty for this offence is five years' imprisonment.

A 2017 landmark Supreme Court judgment broadly interpreted the boundaries of the term "intrusion into computerized material" to cover any access to a computer absent of the owner's permission or some other legal authority. Prosecutions of this offence are becoming more abundant, such as with disgruntled former employees hacking into their former employer's systems, hackers hacking into web-connected cameras, terrorism-oriented hacking and bank account hacking.

Denial-of-service attacks
Denial of service attacks fall within the scope of Section 2 of the Israeli Computers Law, which penalises any obstructions to the ordinary operation of a computer or interference with its use. The maximum penalty for this offence is three years' imprisonment.

Phishing
Phishing falls within the scope of two traditional offences codified in the Israeli Penal Law, 5737-1977, the first being receipt of something by fraud (Section 415 of the Penal Law). This offence is punishable by a maximum term of three years in prison, but if the offence is committed in aggravating circumstances, the maximum punishment is five years in prison. The second offence is receipt of something by ploy or by intentional exploitation of another person's mistake (Section 416 of the Penal Law), punishable by two years' imprisonment. These offences have been the subject of indictments such as online bank account phishing and Facebook account phishing.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Section 6 of the Israeli Computers Law criminalises the programming or adaptation of a computer program for the purpose of unlawfully performing any one of six enumerated acts. Among the enumerated acts is interfering with the ordinary operation of a computer, impacting the integrity of computerised content, facilitating unlawful intrusion into computers or invading a person's privacy. This offence is punishable by up to three years' imprisonment. The act of trafficking in or installing such computer programs is punishable by up to five years in prison. Developers and distributers of spyware, worms, trojans and viruses have been prosecuted under these provisions.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The installation of software or other tools used to commit cybercrime is an offence under Section 6 of the Israeli Computers Law. This also applies to hardware with a firmware component. While mere possession is likely not an offence, it may amount to an attempt to commit the offence. An attempt is punishable by the same prison term prescribed for the completed offence.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft or identity fraud can give rise to two traditional offences codified in the Israeli Penal Law, 5737-1977 – receipt of something by fraud and receipt of something by ploy, both discussed above. In addition, using the identity credentials of another person can give rise to the offence of impersonating another person with intent to defraud, codified in Section 441 of the Israeli Penal Law and punishable by up to three years in prison.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft can give rise to the traditional offence of larceny codified in the Israeli Penal Law, punishable by up to three years in prison, or up to seven years if the stolen property is valued at ILS 500,000 or more. Theft by an employee is a more egregious offence, punishable by up to seven years' imprisonment. If the theft involves data whose confidentiality was compromised by the theft, and the confidentiality arises from an obligation under law, the theft amounts to a criminal invasion of privacy punishable by up to five years' imprisonment.

Copying, importing, renting out or distributing infringing copies of copyrighted material, as well as possession of such copies for the purpose of trafficking are offences under the Israeli Copyright Law, 5768-2007 if they are committed in a commercial scope. These are punishable by up to five years' imprisonment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Other activities that adversely affect or threaten the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data are likely captured by the above offences.

Failure by an organisation to implement cybersecurity measures

Under the Israeli Protection of Privacy Law, 5741-1981, certain organisations are required to appoint an information security officer. Details can be found in the answer to question 4.2 below. Under Section 31A(a)(6) of the Israeli Protection of Privacy Law, failure to appoint an information security officer where such is mandated by the law is a strict lability offence punishable by up to one year in prison.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The above offences have extraterritorial application in three main scenarios. First, if the offence was only partially committed outside Israel, the conduct will be fully captured by the above offences.

Second, if preparations to commit the offence, an attempt to commit it, inducement of another to commit the offence, or conspiracy to commit the offence were performed outside Israel, but the completed offence would have been committed in whole or in part in Israel, then the conduct will be fully captured by the above offences.

Finally, where an offence was committed outside Israel but was targeted against the State of Israel in the broad sense of the phrase (e.g., against national security, the State's regime, the State's property or economy), or was committed by an Israeli resident or citizen, then the conduct will be fully captured by the above offences.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The traditional affirmative defences to criminal culpability also apply to these offences. These defences include necessity, duress and self-defence, yet the bar is rather high to meet. Additionally, both prosecutorial discretion and sentencing guidelines would take into account mitigating factors such as the severity of the conduct, the degree of wilfulness, the scope of harm or affected victims, the motives, etc.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Several other criminal offences which in themselves are not specific to cybersecurity have been used to indict defendants in Israel. Under the specific circumstances of those cases, those charges were applied to cybersecurity matters or to Incidents.

In a recent case, the State of Israel indicted a former employee of an Israeli cyber company in the cyber intelligence business. The defendant was charged with misappropriating intellectual property (cyber and espionage software) and attempting to sell it for $50 million over the Darknet, in a manner potentially harmful to national security. He was also indicted for an attempt to damage property aimed at impairing national security, an offence under section 108 of the Penal Law, and for marketing export-controlled materials without a defence marketing licence, an offence under section 32 of the Defense Export Control Law, 5767-2007.

In the criminal case of *Israel v. Abu Atza*, the defendant was accused of breaking into a victim's car and stealing her handbag, which contained her smartphone. He allegedly published intimate photos of her which he found on her phone, posting them on her own Instagram account. He was also indicted for sexual harassment, an offence under section 3 of the Prevention of Sexual Harassment Law, 5758-1998.

In the case of *Israel v. Oyda*, the defendant, a resident of the Gaza Strip, used software named "Website Hacking" to access the Israeli Police's website and display live streams of traffic cameras in order to gather intelligence against the State of Israel. The defendant had also accessed drone telecommunications for these purposes. He was also indicted with and convicted of membership and activity in an illegal organisation, an offence under section 85 of the Defense Regulations, and espionage, an offence under section 112 of the Penal Law.

In the case of *Israel v. Massrawa*, the defendant used usernames and passwords he collected through a phishing scam, in order to access victim's bank accounts and transfer funds from those accounts. He was also indicted with and convicted of money laundering, an offence under section 3 of the Prohibition on Money Laundering Law, 5760-2000.

In the case of *Israel v. Mualem* (decided on June 30, 2016), the defendant installed monitoring software called "SpyPhone" on personal phones of victims, at the requests of private investigators. The defendant was charged with and convicted of assisting wiretapping without proper authority, an offence under section 2 of the Wiretap Law.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Laws applicable to cybersecurity include the Israeli Computers Law, the Protection of Privacy Law, the Penal Law, the Defense Export Control Law, the Regulation of Security in Public Bodies Law, and the recently proposed Cyber Defense and National Cyber Directorate Bill.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to organisations operating critical infra-

structures on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecom and internet providers, transportation carriers, the Tel Aviv Stock Exchange, the Israeli Internet Association, utility companies and others.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Aside from the cybersecurity requirements applicable to critical infrastructures as explained in the preceding question, the Protection of Privacy Regulations (Data Security), 5777-2017, is an omnibus set of rules. It requires any Israeli organisation that owns, manages or maintains a database containing personal data to implement prescriptive security measures, whose main objective is the prevention of Incidents. These include, for example, physical security measures, access control measures, risk assessment and penetration tests. The regulations classify databases into four categories (basic, intermediate, high and those held by individuals), with each subject to an escalating set of information security requirements.

The regulations also require organisations to monitor and document any event that raises suspicion of compromised data integrity or unauthorised use of data.

Additionally, organisations that hold certain sensitive information are required under the data security regulations to implement an automated audit mechanism to monitor any attempt to access information systems that contain personal data. Sensitive information covers information regarding an individual's private affairs, including: individuals' behaviour in the private domain; health or mental condition; political opinions or religious beliefs; criminal history; telecommunication meta data; biometric data; financial information regarding individuals' assets, debts and economic liabilities; and consumption habits of an individual which may be indicative of the above-mentioned types of data.

In addition, financial institutions and insurance companies are required to operate a security operation centre tasked with monitoring, detecting and mitigating cybersecurity risks.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Use of certain information security measures may constitute telecommunication wiretapping or invasion of privacy. The Israeli Protection of Privacy Law prescribes a number of affirmative defences to invasion of privacy, which are arguably invokable in case of a conflicting legal requirement. Additionally, Section 64 of the proposed Cyber Defense and National Cyber Directorate Bill proposes an exemption from liability for unlawful wiretapping, invasion of privacy, or intrusion into computers, if an organisation takes steps in furtherance of cybersecurity, maintains a cybersecurity policy and is transparent to affected individuals about its use of cybersecurity measures.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There are several provisions according to which certain organisations are required to report Incidents.

First, under the Israeli data security regulations, any organisation that is subject to the intermediate security level or the high security level is required to notify the Protection of Privacy Authority (the Israeli privacy regulator) of the Incident. The notification must state the measures taken to mitigate the Incident. The Protection of Privacy Authority is vested with investigative powers and can request and obtain additional information accessible to the organisation about the Incident, including malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology.

The intermediate security level applies to public agencies, organisations that hold sensitive information and data brokers. The high security level applies to organisations that hold sensitive information or data brokers, in each case of at least 100,000 data subjects or with more than 100 persons with access credentials.

Second, financial institutions and insurance companies are required to report Incidents pursuant to regulatory guidelines by the Israeli Banking Regulator, and insurance companies are required to report to the Israel's Capital Market, Insurance and Savings Authority within the Ministry of Finance.

Third, under the Cyber Defense and National Cyber Organization Bill, the National Cyber Organization and the Israeli Security Agency (colloquially known as the Shin Bet) can approach any organisation in Israel and demand any document and information it has relating to an Incident, instruct the organisation on how to operate its IT system and seize computers, communication systems and drives containing data.

There are no formally specified defences or exemptions by which an organisation might prevent publication of information relating to an Incident.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Voluntarily sharing information about an Incident with the Israeli privacy regulator is a permissible practice that the Israeli privacy regulator encourages in the present cybersecurity landscape. If the Incident eventually turns out to be one for which a notification to the regulator was required, the Israeli privacy regulator will tend to view the voluntary early disclosure as a mitigating factor in regulatory action it might take.

Sharing information about an Incident with a foreign authority is the *de facto* result of non-Israeli data breach notification laws with a long reach, such as the GDPR and state data breach notification laws in the United States.

Finally, sharing information about an Incident with other private sector organisations or trade associations in Israel raises anti-trust issues, but is conditionally permissible pursuant to the Anti-Trust Commissioner's opinion from 2017, if the information shared does not pertain to the business activities of the organisation.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

In certain circumstances, the Israeli privacy regulator may order the organisation after consultation with the Head of the National Cybersecurity Authority, to report the Incident to all affected data subjects. No test case has triggered this to date and thus the particulars of this issue are not yet known.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The data breach notification obligation, as applied by the Israeli data security regulations, depends on the database's security level, which in turn depends on the nature of the information it stores. See the answer to question 2.5 for more information. Yet if the breached data is not capable of identifying an individual, then the Incident need not be reported, since it does not pertain to regulated "personal data".

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Israeli privacy regulator is responsible for enforcing the data security regulations. The Banking Supervisor at the Bank of Israel is responsible for enforcing the data breach rules relating to Incidents in banks and credit card companies. The Supervisor of Capital Markets, Insurance and Savings within the Israeli Ministry of Finance is responsible for enforcing the data breach rules relating to Incidents at insurance companies.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There are currently no penalties imposable by the Israeli privacy regulator for failing to comply with the data breach notification requirement. A proposed amendment to the Israeli Protection of Privacy Law would empower the regulator with authority to impose penalties.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In 2017, the Israeli privacy regulator investigated a data breach revealed in an Israeli company in the business of vehicle location monitoring. The data breach was revealed by an anonymous hacker, who exploited a security vulnerability in the company's website. The regulator launched enforcement action against the company and concluded that it had violated the Israeli data security regulations by not providing a timely notice to the regulator about the Incident.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Use of beacons could arguably amount to unlawful intrusion into computer material but could be defensible under the affirmative defences of necessity or self-defence.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Use of honeypots for detection purposes is likely permissible so long as it does not involve unlawful intrusion into the cyber threat actors' computers or invasion of their privacy (although these may in turn be defensible under the affirmative defences of necessity or self-defence). Use of honeypots for counter-attacks would amount to unlawful unlawful intrusion into the cyber threat actors' computers and other correlative offences.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Use of sinkholes for deflection purposes is likely permissible so long as it does not involve unlawful intrusion into the another person's computer, invasion of their privacy or interference with the ordinary functioning of their computer (although these may in turn be defensible under the affirmative defences of necessity or self-defence).

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Among those considered to be investing the most resources in cybersecurity are banks and credit card companies. This is likely due to them operating in a heavily regulated environment with a highly risk-averse regulator. At the other end of the spectrum are many small and medium businesses that often lack the resources for or awareness to, cybersecurity and compliance with the Israeli data security regulations.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Banks and credit card companies are subject to the cybersecurity requirements laid down by the Supervisor of Banks at the Israeli Central Bank. One of the operative requirements for banking corporations and credit card companies is to appoint a cyber-defence manager and define the board of directors' responsibilities in this realm. They are required to continuously examine the effectiveness of the various cyber-defence controls that they have established – using tools such as vulnerability reviews and controlled-intrusion tests.

Insurance companies and investment firms are subject to the cybersecurity requirements laid down by the Supervisor of Capital Markets, Insurance and Savings. They are required, for instance, to approve, at least once a year, a corporate policy on cybersecurity risk management. They must appoint a chief cybersecurity officer and conduct an annual assessment of the suitability of defensive measures to the organisation's overall cybersecurity risks.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to telecom organisations operating critical infrastructures on matters related to information security and cybersecurity. These directives are not published.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There has yet to develop any Israeli case law on the issue of directors' liabilities relating to cybersecurity, but directors' negligence on cybersecurity governance could amount to a breach of the directors' duty of care. Additionally, cybersecurity guidelines issued by the Supervisor of Banks and the Supervisor of Capital Market, Insurance and Savings do specifically impose duties of oversight on the board of directors of these covered entities. Failure to so do may amount to the directors breaching their duty of care.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the Israeli Protection of Privacy Law, certain organisations are required to appoint an information security officer. These organisations include public agencies, service providers who process five or more databases of personal data by commission for other organisations and organisations that are engaged in banking, insurance and credit evaluation.

Organisations that are subject to the Israel data security regulations must establish and maintain procedures for Incident response.

Organisations that are subject to the intermediate or high security levels under the data security regulations are required to perform cyber risk assessments. Organisations that are subject to the high security level are also required to conduct assessments to identify cybersecurity risks.

Any organisation that is subject to the data security regulations is required to oversee and supervise its vendors' data security compliance on an annual basis.

Finally, organisations that are subject to the high level of security are required to perform penetration tests once every 18 months.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

All publicly traded companies are required to include in their periodic reports details of all types of risks that the company is exposed to in light of their line of business, the environment in which they operate and the characteristics unique to their operations. The Israeli Securities Authority recently published a circular emphasising a public company's duties of disclosure both of general cybersecurity risks that a company faces as well as of specific Incidents having material adverse effects on the company. Research conducted two years ago found that nearly half of the top 125 companies trading on the Tel Aviv Stock Exchange did not report cybersecurity as a risk.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

We are not aware of any other requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The most prominent civil action that may be brought against a legal entity in relation to an Incident is class action lawsuit in accordance with the Israeli Class Action Law, 5766-2006.

In order for the court to certify a class action suit, the representative plaintiff must prove that: (1) the action raises substantive questions of fact or in law common to all members of the putative class that were affected by the Incident, and that it is reasonably possible that such questions will be resolved in the class's favour; (2) under the circumstances of the case, a class action is the efficient and fair method to dispose of the dispute; (3) there are reasonable grounds to assume that the interests of all members of the class will be appropriately represented and conducted; and (4) there are reasonable grounds to assume that the interest of all members of the group will be represented and conducted in good faith.

In addition, any person or legal entity that suffered damages related to an Incident may assert a personal civil action based on several applicable laws; for example – invasion of privacy in accordance with the Protection of Privacy Law or for negligence in accordance with the Israeli Torts Ordinance.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The Incident involving the vehicle monitoring company described in the answer to question 2.11 above has led to at least two class action suits filed against the company, alleging that the company negligently failed to safeguard consumer information.

In September 2017, a similar class action lawsuit was filed against Leumi Card Ltd., an Israeli credit card issuer, following a severe Incident in 2014 where former company employees had stolen vast amounts of information on credit card holders and tried to extort millions of shekels from the company. The class action lawsuit alleges that the company negligently failed to safeguard consumer information.

In April 2011, the Herzliya Magistrate Court awarded ILS 400,000 to a plaintiff for damages he suffered after the defendants infected his personal computer with a Trojan in the wake of a family dispute.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A person or entity responsible for safeguarding data against an Incident may arguably be liable in tort for failing to take the security measures required under the Israeli data security regulations in negligence or the tort of breach of a legal duty.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents, and it is in fact becoming more common.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no noteworthy regulatory limits.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Israeli legislation does not specifically address the issue of monitoring and accessing employees' communications and files. This legislative gap has been filled by case law, the most notable being a judgment delivered by the Israeli National Labor Court in 2011, known as the Isakov case. The judgment expounded Israeli privacy law as applied to employers monitoring and accessing employees' communications and files. The decision sets forth the boundaries of permissible access to employee's email communications. The ruling also sets forth a stringent set of pre-requisites and conditions for permissible access.

There are no specific requirements under Applicable Law regarding the reporting of cyber risks or Incidents by employees. Such requirements can be contractually stipulated in an employment agreement. Arguably, they can also be interpreted, in appropriate circumstances, to be part of an employee's general fiduciary obligations towards the employer or part of an employee's duty to act in good faith.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

We are not aware of any such laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Israeli Police is empowered with general authority to investigate crimes and to seize documents, objects and computer materials that can potentially serve as evidence relating to the commission of a crime. Seizure of computers and computer material used by a business for investigation purposes requires a court order.

The Israeli privacy regulator has investigative powers relating to violations of the Israeli Protection of Privacy Law, including issues relating to the cybersecurity of databases containing personal data.

The Israeli Wiretap Law authorises investigative and security authorities to surreptitiously obtain the content of real time communications, for national security purposes or for the purpose of preventing and investigating serious crime. Wiretaps sought for preventing and investigating serious crime are subject to court approval, which in exceptional cases can be sought after the fact.

The Israeli Telecom Data Law provides police and various other investigative bodies with the authority to apply to the court of lowest instance in Israel to seek a comprehensive order to surreptitiously receive metadata (but not the content) of telecommunications, for the purpose of search and rescue, investigating or preventing crime, or seizing property. If metadata is required urgently and a court order cannot be obtained in time, such metadata may be obtained for a limited period of 24 hours, without a court order, subject to approval by a senior police officer.

Recently, a proposal for a Cyber Defense and National Cyber Directorate Bill was published. It proposes granting far-reaching and unprecedented powers to the National Cyber Directorate, such as compelling organisations to produce any information or document required to handle cyber-attacks and authority to issue instructions to organisations, including instructions to carry-out acts on the organisation's computerised material, for the purpose of handling cyber-attacks.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Section 11 of the General Security Service Law, 5762-2002 (the statute governing the operation of the Israeli Security Agency, colloquially known as "Shabak" or "Shin Bet"), grants the Prime Minister sweeping powers to order that metadata and non-real time

telecommunications be retained by telecom providers and surreptitiously made available to the Shabak.

Section 13 of the Communications Law (Telecommunication and Broadcasts), 5742-1982, provides that the Prime Minister may order telecom service providers to render services to police, security agencies and intelligence agencies, and to have the providers install devices, take measures or adapt their facilities to assist the authorities.

Haim Ravia is a Senior Partner and Chair of the Internet, Cyber and Copyright Practice Group at Pearl Cohen Zedek Latzer Baratz. Haim deals extensively with data protection and privacy, cyber and internet law, IT contracts, copyright, electronic signatures, and open source software. Haim was a member of the Israeli public commission for the Protection of Privacy, and was part of a governmental team that re-examined the Israeli law pertaining to personal information databases. Haim received an acknowledgment award from the Israel Chamber of Information System Analysts for pioneering and innovation in the Israeli internet. Practising internet and cyber law for over 20 years, Haim has also written numerous columns on internet law for *Globes* (a major Israeli financial newspaper), the *Israel Bar Association Magazine* and other publications. Haim also operates Israel's first legal website (www.law.co.il) and publishes commentaries on *Lexology*.

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9058
Fax: +972 3 303 9001
Email: HRavia@PearlCohen.com
URL: www.pearlcohen.com
www.law.co.il

Dotan Hammer is a Partner and member of the Internet, Cyber and Copyright Group at Pearl Cohen Zedek Latzer Baratz. Dotan regularly advises on Israeli data protection and privacy laws. Having completed his academic degree in computer science at the age of 19, later working as a software developer and a technological project leader, Dotan also counsels clients on the privacy and data protections aspects of software and SaaS user agreements and licensing, as well as on other IT law matters such as digital (electronic) signatures, copyright issues and open source matters. Dotan regularly contributes to Israel's first legal website (www.law.co.il), *Lexology* and other online publications.

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9037
Fax: +972 3 303 9001
Email: DHammer@PearlCohen.com
URL: www.pearlcohen.com
www.law.co.il

Japan

Mori Hamada & Matsumoto

Hiromi Hayashi

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

As background, there are two main laws criminalising cyber attacks, namely (A) the Act on the Prohibition of Unauthorized Computer Access (the "**UCAL**"), and (B) the Penal Code.

(A) The UCAL imposes criminal sanctions on any person who makes an Unauthorized Access to a computer (an "**Access Controlled Computer**"), the access to and operation of which are under the control of an administrator (the "**Access Administrator**").

An "Unauthorized Access" means any action which operates an Access Controlled Computer by either (i) inputting an identification code (*shikibetsu-fugou*) (e.g., password and ID) allocated to a user who is authorised to access the Access Controlled Computer (an "**Authorized User**"), without the permission of the Access Administrator or the Authorized User, or (ii) inputting any information (other than an identification code) or command which enables that person to evade control (e.g., cyber attack of a security flaw), without the permission of the Access Administrator (UCAL, Article 2, Paragraph 4).

The UCAL prohibits the following actions:

(a) an Unauthorized Access (Article 3);

(b) obtaining the identification code of an Authorized User to make an Unauthorized Access (Article 4);

(c) providing the identification code of an Authorized User to a third party other than the Access Administrator or the Authorized User (Article 5);

(d) keeping the identification code of an Authorized User which was obtained illegally to make an Unauthorized Access (Article 6); and

(e) committing the following acts by impersonating the Access Administrator or causing a false impression of being the Access Administrator by: (a) setting up a website where the fake Access Administrator requests an Authorized User to input his/her identification code; or (b) sending an email where the fake Access Administrator requests an Authorized User to input his/her identification code (Article 7).

Any person who commits (a) above (Article 3) is subject to imprisonment of up to three years or a fine of up to JPY 1,000,000 (Article 11). Any person who commits (b) to (e) above (Articles 4 to 7) is subject to imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12). However, if the person committing (c) (Article 5) does not know that the recipient intends to use the identification code for an Unauthorized Access, that person is subject to a fine of up to JPY 300,000 (Article 13).

(B) The Penal Code provides for criminal sanctions on the creation and provision of Improper Command Records which give improper commands, such as a computer virus, to a computer (*fusei shirei denji-teki kiroku*). "**Improper Command Records**" mean (i) electromagnetic records that give a computer an improper command which causes the computer to be operated against the operator's intention or fail to be operated in accordance with the operator's intention, and (ii) electromagnetic or other records which describe such improper commands.

Under the Penal Code, any person who creates or provides, without any justifiable reason, Improper Command Records, or who knowingly infects or attempts to infect a computer with Improper Command Records, is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Article 168-2). Any person who obtains or keeps Improper Command Records for the purpose of implementing such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Article 168-3).

In addition, the Penal Code provides for the following additional penalties:

(i) any person who obstructs the business of another by causing a computer used in the business to be operated against the operator's intention, or fail to be operated in accordance with the operator's intention, by (a) damaging that computer or any electromagnetic record used by that computer, or (b) giving false information or an improper command to the computer is subject to imprisonment of up to five years or a fine of up to JPY 1,000,000 (Article 234-2);

(ii) any person who gains or attempts to gain, or causes or attempts to cause a third party to gain, illegal financial benefits by (a) creating false electromagnetic records by giving false information or an improper command to a computer, or (b) providing false electromagnetic records for processing by a third party, in either case, in connection with a gain, a loss or a change regarding financial benefits is subject to imprisonment of up to 10 years (Article 246-2); and

(iii) any person who creates, provides or attempts to provide electromagnetic records for the purpose of causing a third party to mistakenly administer matters which relate to rights, obligations or proofs of facts is subject to imprisonment of up to five years or a fine of up to JPY 500,000. However, if the act relates to records to be made by public authorities or public servants, the penalty is imprisonment of up to 10 years or a fine of up to JPY 1,000,000 (Article 161-2).

Hacking is an Unauthorized Access under the UCAL, punishable by imprisonment of up to three years or a fine of up to JPY 1,000,000.

If the hacking is made through Improper Command Records, it is also punishable under the Penal Code (please see question 1.1(B) above). In addition, if a business is obstructed by such hacking, the crime is punishable by imprisonment of up to five years or a fine of up to JPY 1,000,000 (Penal Code, Article 234-2).

Denial-of-service attacks
This carries the same penalties as hacking.

Phishing
Article 7 of the UCAL prohibits phishing, while Article 4 of the UCAL prohibits obtaining any identification code through phishing. These actions are punishable by imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12).

In addition, any person who gains illegal benefits by using identification codes obtained by phishing is subject to imprisonment of up to 10 years under Article 246-2 of the Penal Code.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This carries the same penalties as hacking.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Any person who obtains or keeps Improper Command Records for the purpose of using such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Penal Code, Article 168-3).

As an example, nine persons were prosecuted for uploading software which contained a computer virus to an online storage system, and which infected the computers of people who accessed the storage and downloaded the software from September to December 2016.

Identity theft or identity fraud (e.g. in connection with access devices)
This carries the same penalties as phishing.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
In addition to the criminal penalties applicable to phishing, electronic theft is penalised under the Unfair Competition Prevention Act. If a current or former employee (a) acquires a trade secret of the employer through theft, fraud, threat or other illegal actions (the "**Illegal Actions**"), including an Unauthorized Access, or (b) uses or discloses a trade secret of the employer acquired through Illegal Actions, for the purpose of obtaining wrongful benefits or damaging the owner of the trade secret, that employee is subject to imprisonment of up to 10 years or a fine of up to JPY 20,000,000, or both (Article 21, Paragraph 1). In addition, if that employee commits any of the foregoing acts outside Japan, the fine is increased up to JPY 30,000,000 (Article 21, Paragraph 3).

Under the Copyright Act, any person who uploads electronic data of movies or music, without the permission of the copyright owner, to enable another person to download them is subject to imprisonment of up to 10 years or a fine of up to JPY 10,000,000, or both (Article 119, Paragraph 1). Furthermore, any person who downloads electronic data which is protected by another person's copyright, and who knows of such protection, is subject to imprisonment of up to two years or a fine of up to JPY 2,000,000, or both (Article 119, Paragraph 3). In addition, any person who sells, lends, manufactures, imports, holds or uploads any device or program which may remove, disable or change technology intended to protect copyright (e.g., copy protection code) is subject to imprisonment of up to three years or a fine of up to JPY 3,000,000, or both (Article 120-2).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
This carries the same penalties as electronic theft.

Failure by an organisation to implement cybersecurity measures
The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorized Users, examine the validity of functions to control access to the Access Controlled Computer and to implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes which have not been used for a long time, implementing a batch program to address a security hole, program updates and appointing an officer for network security) (Article 8). However, there is no criminal sanction on a breach of these obligations.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The UCAL provides for the extraterritorial application of Articles 3, 4, 5 (except where the offender did not know the recipient's purpose) and 6 of the UCAL (Article 14).

The Penal Code also has extraterritorial application (Article 4-2).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

No, there are no such actions.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

No. The Organized Crime Act, which applies to an act of terrorism, designates certain material crimes, such as murder, identified in the Penal Code and imposes penalties which are heavier than those under the Penal Code. However, criminal offences regarding cybersecurity, which are described in question 1.1 above, are not designated crimes under the Organized Crime Act.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

In addition to the UCAL, the Penal Code and the Unfair Competition Prevention Act described above, the following laws are also applicable to cybersecurity.

- Basic Act on Cybersecurity
  This provides the basic framework for the responsibilities and policies of the national and local governments to enhance

cybersecurity. Furthermore, it obligates operators of material infrastructure (e.g., financial institutions, operators of railroads, airplanes and other means of transportation and providers of electricity, gas and water) and networks (e.g., telecommunications networks) to make efforts to voluntarily and proactively enhance cybersecurity, and to cooperate with the national and local governments to promote measures to enhance cybersecurity. Based on this Basic Act, the National Center of Incident Readiness and Strategy for Cybersecurity was established in 2015.

The Basic Act, which provides for the establishment of a cybersecurity council ("**Cybersecurity Council**"), was approved by the Diet in December 2018. The Cybersecurity Council is intended to be the avenue to allow national and local governmental authorities and business operators to share information which may facilitate the proposal and implementation of cybersecurity measures. The Cybersecurity Council was established in April 2019.

- Telecommunication Business Act (the "**TBA**")

  Article 4 of the TBA provides that (1) the secrecy of communications being handled by a telecommunications carrier shall not be violated, and (2) any person who is engaged in a telecommunications business shall not disclose secrets obtained while in office, with respect to communications being handled by the telecommunications carrier, even after he/she has left office. The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, data on access logs and IP addresses are protected under the secrecy of communications. If a telecommunications carrier intentionally obtains any information protected under the secrecy of communications, discloses protected information to third parties and uses protected information without the consent of the parties who communicated with each other, that telecommunications carrier is in breach of Article 4(1).

  To prevent cyber attacks, it would be useful for telecommunications carriers to collect and use information regarding cyber attacks, e.g., access logs of infected devices, and share this information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyber attacks without breaching Article 4(1). The Ministry of Internal Affairs and Communications ("**MIC**"), the governmental agency primarily responsible for implementing the TBA, issued reports in 2014, 2015 and 2018 which addressed whether a telecoms carrier may deal with cyber attacks and the issues that may arise in connection with the secrecy of communications. The findings of the three reports are included in the guidelines on cyber attacks and the secrecy of communications (the "**Guidelines**"), issued by the Council regarding the Stable Use of the internet. The Council is composed of five associations which are the ICT Information Sharing And Analysis Center Japan, the Telecommunications Carriers Association, the Telecom Services Association, the Japan Internet Providers Association and the Japan Cable and Telecommunications Association. The Guidelines include the contents of MIC's three reports. The Guidelines, however, are not legally binding, although they carry a lot of weight because MIC confirmed them before the Guidelines were issued.

  Furthermore, in 2013, MIC started a project called ACTIVE (Advanced Cyber Threats response InitiatiVE) that aims to protect internet users from cyber attacks by collaborating with ISPs and vendors of IT systems. To prevent computer virus infections, warning users or blocking communications in accordance with the Guidelines may be done by ISPs which are members of ACTIVE.

  In addition, in May 2018, the TBA was amended to introduce a new mechanism which enables a telecommunications carrier to share with other carriers information on transmission sources of cyber attacks through an association which MIC confirms is eligible to assist telecommunications carriers. After the amendments became effective in November 2018, MIC designated ICT Information Sharing And Analysis Center Japan to be that association in January 2019.

- Act on the Protection of Personal Information (the "**APPI**")

  The APPI is the principal data protection legislation in Japan. It is the APPI's basic principle that the cautious handling of Personal Information under the principle of respect for individuals will promote the proper handling of Personal Information. "**Personal Information**" means information about specific living individuals which can identify them by name, date of birth or other descriptions contained in the information (including information that will allow easy reference to other information, which may enable individual identification) (Article 2, Paragraph 1). A business operator handling Personal Information may not disclose or provide Personal Information without obtaining the subject's consent, unless certain conditions are met.

  To prevent cyber attacks, it would be useful for business operators to collect and use information regarding the cyber attacks, e.g., access logs of infected devices, and share this information with other business operators or public authorities. However, if the information includes Personal Information, it would be subject to the restrictions on the use and disclosure of Personal Information under the APPI.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorized Users, examine the validity of functions to control access to the Access Controlled Computer and implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes which have not been used for a long time, implementing a batch program to address a security flaw, program updates and appointing an officer for network security) (Article 8).

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Ministry of Economy, Trade and Industry ("**METI**") and the Independent Administrative Agency Information-technology Promotion Agency ("**IPA**") jointly issued the Cybersecurity Management Guidelines (the latest version of which is as of November 2017). The guidelines describe three principles that the management of companies, which have a dedicated division for information system and are utilising IT, should recognise to protect their company from cyber attacks and 10 material items on which management should give instructions to executives or directors in charge of IT security, including the chief information security officer ("**CISO**").

The 10 material items and some examples of recommended actions for each item described in the guidelines are as follows:

(i) Recognise cybersecurity risks and develop company-wide measures.
Example: Develop a security policy which incorporates cybersecurity risk management while aligning it with the company's management policy, so that management can publish company-wide measures.

(ii) Build a structure or process for cybersecurity risk management.
Example: CISO to establish a system to manage cybersecurity risks and set forth the responsibilities clearly.
Example: Directors to examine whether a system which will manage cybersecurity risks has been established and is being operated properly.

(iii) Secure resources (e.g., budget and manpower) to execute cybersecurity measures.
Example: Allocating resources to implement specific cybersecurity measures.

(iv) Understand possible cybersecurity risks and develop plans to deal with such risks.
Example: During a business strategy exercise, identify information which needs protection and cybersecurity risks against that information (e.g., damage from leakage of trade secrets on a strategic basis).

(v) Build a structure to deal with cybersecurity risks (i.e., structure to detect, analyse and defend against cybersecurity risks).
Example: Secure the computing environment and network structure used for important operations by defending them through multiple layers.

(vi) Publish a cybersecurity measures framework ("**PDCA**") and its action plan.
Example: Develop a structure or process where one can constantly respond to cybersecurity risks (assurance of implementation of PDCA).

(vii) Develop an emergency response system (emergency contacts, initial action manual and Computer Security Incident Response Team ("**CSIRT**")) and execute regular hands-on drills.
Example: Issue instructions to promptly cooperate with relevant organisations and to investigate relevant logs to ensure that efficient actions or investigations can be taken to identify the cause and damage of a cyber attack.
Example: Execute drills, including planning activities, to prevent recurrence after Incidents and reporting Incidents to relevant authorities.

(viii) Develop a system to recover from the damages caused by an Incident.
Example: Establish protocols for recovery from business suspension, or other damages caused by an Incident, and execute drills in accordance with these protocols.

(ix) Ensure that entities in the company's entire supply chain, including business partners and outsourcing companies for system operations, take security measures.
Example: Conclude agreements or other documents to provide clearly how group companies, business partners and outsourcing companies for system operations in the company's supply chain will take security measures.
Example: Have access to and understand reports on how group companies, business partners and outsourcing companies for system operations in the company's supply chain take security measures.

(x) Collect information on cyber attacks through participation in information-sharing activities and develop an environment to utilise such information.
Example: Help society guard against cyber attacks by actively giving, sharing and utilising relevant information.
Example: Report information on malware and illegal access to the IPA in accordance with public notification procedures (standards for countermeasures for computer viruses and for illegal access to a computer).

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The secrecy of communications is strongly protected under the TBA. To prevent cyber attacks, it would be useful for telecommunications carriers to collect and use information regarding the cyber attacks, e.g., access logs of infected devices, and share this information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyber attacks without breaching Article 4(1). Thus, it is difficult for telecommunications carriers to balance the prevention of cyber attacks with the protection of secrecy of communications. MIC tried to deal with this issue by helping to establish the Guidelines and by amending the TBA to introduce a new mechanism to share information on transmission sources of cyber attacks (please see question 2.1 above).

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no mandatory requirement to report Incidents.

However, under the guidelines for banks issued by the Financial Services Agency ("**FSA**"), banks are required to report an Incident immediately after becoming aware of it. The guidelines are not legally binding; however, because FSA is a powerful regulator of the financial sector, banks would typically comply with FSA's guidelines (please see question 3.1). The report must include:

(i) the date and time when the Incident occurred and the location where the Incident occurred;
(ii) a summary of the Incident and which services were affected by the Incident;
(iii) causes of the Incident;
(iv) a summary of the facilities affected by the Incident;
(v) a summary of damages caused by the Incident, and how and when the situation was remedied or will be remedied;
(vi) any effect to other business providers;
(vii) how the banks responded to enquiries from users and how they notified users, public authorities and the public; and
(viii) possible measures to prevent similar Incidents from happening.

In addition, if a cyber attack causes a serious Incident specified in the TBA and the enforcement rules of the TBA, such as a temporary suspension of telecommunications services or a violation of the secrecy of communications, the telecommunications carrier is required to report the Incident to MIC promptly after its occurrence. In addition, the carrier is required to report the details of the said Incident to MIC within 30 days from its occurrence. The detailed report must include:

(i) the date and time when the Incident occurred;

(ii) the date and time when the situation was remedied;
(iii) the location where the Incident occurred (the location of the facilities);
(iv) a summary of the Incident and which services were affected by the Incident;
(v) a summary of the facilities affected by the Incident;
(vi) details of the events or indications of the Incident, the number of users affected and the affected service area;
(vii) measures taken to deal with the Incident, including the persons who dealt with it, in chronological order;
(viii) causes which made the Incident serious, including how the facilities have been managed and maintained;
(ix) possible measures to prevent similar Incidents from happening;
(x) how the telecoms carrier responded to inquiries from users and how it notified users of the Incident;
(xi) internal rules in connection with the Incident;
(xii) if the telecoms carrier experienced similar Incidents in the past, a summary of the past Incidents;
(xiii) the name of the manager of the telecoms facilities; and
(xiv) the name and qualifications of the chief engineer of the telecoms facilities.

Furthermore, it is recommended that companies report the Incident to the IPA (please see question 2.3 above). The report must include:

(i) the location of where the infection was found;
(ii) the name of the computer virus. If the name is unknown, features of the virus found in the IT system;
(iii) the date when the infection was found;
(iv) the types of OS used and how the IT system is connected (e.g. LAN);
(v) how the infection was found;
(vi) possible cause of the infection (e.g., email or downloading files);
(vii) extent of the damage (e.g., the number of infected PCs); and
(viii) whether the infection has been completely removed.

The IPA also has a contact person whom the companies may consult, whether or not they file a report with the IPA, as to how they can deal with cyber attacks or any Unauthorized Access. According to the IPA's website, it had 8,000 consultations in 2018.

If the Incidents involve any disclosure, loss or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the Personal Information Protection Committee (the "**PPC**") regarding the APPI, the operator is expected to promptly submit to the PPC a summary of such disclosure, loss or damage and planned measures to prevent future occurrences.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Please see question 2.1.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The Cybersecurity Management Guidelines recommend knowing who should be notified if a cyber attack has caused any damage, gathering information to be disclosed and promptly publishing the Incident, taking into account its impact on stakeholders (please see question 2.3).

Furthermore, if the Incidents involve any disclosure, loss or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the PPC regarding the APPI, the operator is expected, depending on the contents or extent of the disclosure, loss or damage, to notify the affected individuals of the facts relevant to the disclosure, loss or damage, or to make the notification readily accessible to the affected individuals (e.g., posting the notification on the operator's website) in order to prevent secondary damages or similar Incidents.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, IP addresses and email addresses are protected under the secrecy of communications. Furthermore, personally identifiable information is protected under the secrecy of communications if it is delivered through telecommunications facilities. With respect to an Incident, a telecommunications carrier may not share information protected under the secrecy of communications unless it complies with the Guidelines through a mechanism under the amended TBA or the instructions of ACTIVE (please see questions 2.1 and 2.5).

In addition, personally identifiable information of cyber threat-makers and individuals who have been inadvertently involved in an Incident would be Personal Information under the APPI which cannot be provided to a third party without obtaining the prior consent of the data subjects, except in limited instances. One such exception is where a public authority needs the cooperation of a private person to implement the authority's legal duties, and the performance of those legal duties will likely be impeded if the private person has to first obtain the data subject's consent. In this regard, the provision of personally identifiable information of cyber threat-makers would not require their consent.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

MIC is the governmental agency primarily responsible for implementing the TBA.

METI is not a regulator that has a specific mandated regulatory authority under specific laws. Rather, it promulgates desirable policies for each industry.

The PPC is an independent organ which supervises the enforcement and application of the APPI.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Other than the report of a serious Incident under the TBA (please see question 2.5), reporting is not mandatory. If a telecommunications carrier does not report a serious Incident, it is subject to a fine of up to JPY 300,000.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No examples can be found based on publicly available information.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of beacons is permissible so long as the use complies with the Guidelines and Applicable Laws.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of honeypots is permissible so long as the use complies with the Guidelines and Applicable Laws.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of sinkholes is permissible so long as the use complies with the Guidelines and Applicable Laws.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

In general, the financial business sector and the telecommunications service sector closely collaborate with relevant authorities on information security.

In July 2015, FSA issued a summary of its policies to strengthen cybersecurity in the financial business sector. According to the summary, FSA's five policies are: (i) continuous dialogue with financial institutions to understand their cybersecurity risks; (ii) improving information-sharing among financial institutions; (iii) implementing cybersecurity exercises in which financial institutions, FSA and other public authorities participate; (iv) developing cybersecurity human resources; and (v) establishing a department in FSA to handle cybersecurity matters. Based on these policies, FSA amended its guidelines for banks to include standards on cybersecurity management, such as establishing an organisation to handle emergencies (e.g., CSIRT), designating a manager in charge of cybersecurity, preparing multi-layered defences against cyber attacks and implementing a periodic assessment of cybersecurity. To implement policy (v), FSA established a department to handle cybersecurity in July 2015, and the latest revisions were made to policies (i) through (iv) in October 2018. The guidelines are not legally binding; however, because FSA is a powerful regulator of the financial sector, banks would typically comply with FSA's guidelines.

As described above, telecommunications carriers are required to report a serious Incident specified in the TBA (please see question 2.5). In addition, if a telecommunications carrier does not take appropriate measures to remedy problems with its services, MIC may order it to improve its business. Failure to comply with the order is subject to a fine of up to JPY 2,000,000.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Please see question 3.1.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Under the Companies Act, a director has the duty to act with "due care as a prudent manager" in performing his/her functions as director (*zenkan chuui gimu*). The applicable standard of care is that which a person in the same position and situation would reasonably be expected to observe. In general, if a director fails to get relevant information, enquire or consider how to prevent Incidents, to the extent these acts are reasonably expected of him/her based on the facts when he/she made a decision (e.g., decision to purchase the IT system), then he/she would be in breach of this duty.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Cybersecurity Management Guidelines, jointly issued by METI and IPA, recommend companies to build a structure or process for cybersecurity risk management and, as an example, to designate a

CISO according to the companies' policies, including the security policy (please see question 2.3).

Furthermore, FSA's guidelines for banks provide the standards regarding cybersecurity management, such as establishing an organisation to handle emergencies (e.g., CSIRT), designating a manager in charge of cybersecurity and implementing a periodic assessment of cybersecurity (please see question 3.1).

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no disclosure requirements that are specific to cybersecurity risks or Incidents.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Basically, if a person breaches a contract, the other party may bring a civil action based on the breach. The plaintiff has the burden of proving the breach, the damages incurred by it and the causation between the breach and the plaintiff's damages.

In addition, the Civil Act of Japan provides for a claim based on tort. If a person causes damages to another, the injured party may bring a civil action based on tort. The plaintiff has the burden of proving the damages incurred by it, the act attributable to the defendant and the causation between the defendant's act and the plaintiff's damages.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

A vendor of a computer system was sued by a company which used the system provided by the vendor. The case related to cyber attacks (SQL injections) to the system which resulted in the disclosure of credit card information of the company's clients. The company sought the payment of damages caused by the cyber attacks in the amount of approximately JPY 100,000,000, based on breach of contract. The Tokyo District Court decided that although the vendor was required to provide programs which are suitable for blocking SQL injections in accordance with existing standards when the computer system was provided, the Incident was also partially attributable to the company because it ignored the vendor's proposal to improve the system. The vendor was ordered to pay only approximately JPY 20,000,000 (Tokyo District Court decision dated January 23, 2014).

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Tort theory is available under the Civil Act of Japan (please see question 5.1).

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. In general, there are two categories of insurance against Incidents, namely (i) insurance to cover the losses incurred by the vendor of an IT system, and (ii) insurance to cover the losses incurred by a business operator using the IT system.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations on insurance coverage under the law. The coverage may differ depending on the insurance products of different insurance companies.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No, there are no specific requirements.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are no Applicable Laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcers have the power to investigate Incidents which are related to crimes under Applicable Laws. In accordance with the "cybercrime project" of the National Police Agency, the police in each prefecture have established a contact point where consultations and information regarding cybercrimes are handled.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are no such requirements.

Hiromi Hayashi is a partner at Mori Hamada & Matsumoto, which she joined in 2001. She specialises in communications law and regulation and authored the Japanese portion of Telecommunication in Asia in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. She was admitted to the Bar in 2001 in Japan and in 2007 in New York. She worked at Mizuho Corporate Bank from 1989 to 1994 and at Davis Polk & Wardwell in New York from 2006 to 2007.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Email: hiromi.hayashi@mhm-global.com
URL: www.mhmjapan.com

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in Fukuoka, Nagoya, Osaka, Beijing, Shanghai, Singapore, Yangon, Bangkok and Ho Chi Minh, and a Jakarta desk. The firm has over 450 attorneys and a support staff of approximately 500, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well-known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise on, telecommunications, broadcasting, the Internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

www.mhmjapan.com

MORI HAMADA & MATSUMOTO

Kenya


Hazel Okoth


Stella Ojango

Gikera & Vadgama Advocates

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
The offence of unauthorised access is committed where a person, whether temporarily or permanently, causes a computer system to perform a function by infringing security measures with intent to gain access without authorisation. Access is unauthorised if that person is not entitled to control access of the computer system in question or does not have consent from the person authorised to access the computer system. This offence is punishable by a fine not exceeding Kshs. 5,000,000.00 or to imprisonment for a term not exceeding three years, or both. However, if the unauthorised access is gained with the intent to commit a further offence, the liability on conviction is a fine not exceeding Kshs. 10,000,000.00 or imprisonment for a term not exceeding 10 years, or both.

Denial-of-service attacks
Any person who without lawful authority or lawful excuse does an act which causes a denial of access to any program or data stored in a computer system is liable upon conviction to a fine not exceeding Kshs. 200,000.00 or to imprisonment for a term not exceeding two years, or both.

Phishing
Phishing is described as creating or operating a website or sending a message through a computer system with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorised access to a computer system. The liability on conviction is a fine not exceeding Kshs. 300,000.00 or to imprisonment for a term not exceeding three years, or both.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
See below.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing an offence is liable on conviction to a fine not exceeding Kshs. 20,000,000.00 or to imprisonment for a term not exceeding 10 years, or both.

If a person knowingly receives or is in possession of a program or a computer password, device, access code or similar data procured through any means described above and intends that it be used to commit or assist in the commission of an offence is liable on conviction to a fine not exceeding Kshs. 10,000,000.00 or to imprisonment for a term not exceeding five years, or both.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft and impersonation occurs when a person fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person. This offence is punishable by a fine not exceeding Kshs. 200,000.00 or to imprisonment for a term not exceeding three years, or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The general punishment for stealing anything that is capable of being stolen is imprisonment for three years, unless the circumstances of the theft or the nature of the thing stolen dictates some other punishment.

Breach of confidence by an employee does not constitute a criminal offence, but civil proceedings may be instituted against said employee for breach of contract.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Unauthorised disclosure of password or access code – Knowingly and without authority disclosing any password, access code or other means of gaining access to any program or data held in any computer system. This offence is punishable by a fine not exceeding Kshs. 5,000,000.00 or to imprisonment for a term not exceeding three years, or both.

Failure by an organisation to implement cybersecurity measures
The requirement to implement cybersecurity measures is highest on owners of critical information infrastructure as well as organisations in certain regulated industries. The National Computer and Cybercrimes Co-ordination Committee is tasked with regulating the minimum physical and technical security measures that must be implemented in order to protect critical information infrastructure.

The standard of compliance is therefore high but non-implementation nonetheless does not constitute a criminal offence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Computer Misuse and Cybercrimes Act does provide for international cooperation in addition to the provisions of our Mutual Legal Assistance Act of 2011 and the Extradition (Contiguous and Foreign Countries) Act. The Office of the Attorney General and the Department of Justice may make a request in any criminal matter to a requested state for purposes of undertaking investigations or proceedings concerning offences related to computer systems, collecting evidence of an offence or obtaining expeditious preservation and disclosure of traffic data or real time collection of traffic data. A requesting state may also make a similar request to the Office of the Attorney General and the Department of Justice, which may either be granted or refused. In any case, any act or omission committed outside Kenya which would, if committed in Kenya, constitute an offence is deemed to have been committed in Kenya if the person committing the act or omission is a citizen of Kenya or ordinarily resident in Kenya and the act or omission is committed against a citizen of Kenya, against property belonging to the Government of Kenya outside Kenya, or to compel the Government of Kenya to do or refrain from doing any act, or if the person who commits the act or omission is after its commission or omission present in Kenya.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Whereas the Computer Misuse and Cybercrimes Act does not specifically provide any actions that may mitigate the penalty of an offence or an exception to any offence, the Kenya Criminal Procedure Code provides that a court may before passing sentence or making any order against an accused person, receive such evidence as it thinks fit in order to inform itself as to the sentence or order to be passed or made. Mitigation is a well-established practice of the Kenyan Courts and some of the factors that the court may consider include the cause of the crime, the magnitude of the crime, prevalence and type of crime, aggravating or extenuating circumstances, the circumstances of the accused, any previous convictions as well the uniformity in the approach to sentencing.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

According to the Kenya Prevention of Terrorism Act, No. 30 of 2012, a terrorist act involves among other things the interference with an electronic system resulting in the disruption of the provision of communication, financial, transport or other essential services. A person who commits a terrorist act that results in this Incident or any other Incident elucidated in the Act is liable to imprisonment for a term not exceeding 30 years and if such an act results in the death of another person, such person is liable to life imprisonment.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Over and above the Computer Misuse and Cybercrimes Act*, the Kenya Information and Communications Act is the substantive law with respect to Data Protection in Kenya.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Director to the Secretariat of the National Computer and Cybercrimes Co-ordination Committee is responsible for designating a system as critical infrastructure. Within a reasonable time after such declaration of an information infrastructure as critical, the Director shall issue directives to regulate:

- the classification of data held by the critical information structure;
- the protection, storage and archiving of data held by the critical information infrastructure;
- cybersecurity Incident management by the critical information infrastructure;
- disaster contingency and recovery measures which must be put in place by the critical information infrastructure;
- minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure; and
- the period within which the owner or person in control of a critical information infrastructure must comply with the directives.

The Committee, together with the owner of the critical information infrastructure shall conduct an assessment of the threats and vulnerabilities of a cyber-attack across all critical infrastructure sectors, determine the harm to the economy that would result from damage or unauthorised access to critical infrastructure, measure the overall preparedness of each sector against damage or unauthorised access to critical infrastructure and identify any other risk-based security factors appropriate and necessary to protect public health and safety.

The owner of a critical information infrastructure is required to report to the Committee any Incidents likely to constitute a threat in the nature of an attack that amounts to a cybercrime.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Generally, body corporates shall run their affairs in a manner where the commission of any offence, including a cybercrime, is prohibited in line with the relevant law. This is done by maintaining various policies such as a cybersecurity policy and general data protection regulations.

Organisations in certain regulated industries, for instance the banking industry, are indeed required to maintain a cybersecurity policy in a manner specified by the regulator as well as to adopt other practices to prevent cyber threats and related Incidents.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Conflicts of laws usually do not arise because any cybersecurity guidelines issued in a specific industry stipulate that such guidelines supplement existing legislation and regulations and in case of any conflict the law will prevail.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The owner or operator of a critical information infrastructure is required to report to the National Computer and Cybercrimes Co-ordination Committee any Incident likely to constitute a threat in the nature of an attack that amounts to a computer and cybercrime. Moreover, a person who operates a computer system, whether public or private, shall immediately inform the Committee of any attacks, intrusions and other disruptions to the functioning of a computer system or network within 24 hours of such attack, intrusion or disruption. This report shall include information about the breach, including information on how the breach occurred, an estimate of the number of people affected by the breach, an assessment of the risk of harm to the affected individuals and an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach. The Committee may then propose the isolation of any computer system or network suspected to have been attacked or disrupted pending the resolution of the issues.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

This is not applicable in Kenya.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The report of any cyber threat, intrusion or disruption to the Committee shall include an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach. Organisations therefore have a duty to report any Incidents or potential Incidents to the affected individuals or otherwise proffer an explanation as to why the affected persons cannot be informed.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Any person or body corporate may provide a reasonable explanation for non-disclosure of sensitive or proprietary information if such information falls within the disclosure requirements of an Incident report to the Committee. In any case, the spirit of the Act is to enable the timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cyber-crimes and not to facilitate the disclosure of confidential information.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Over and above receiving and acting on reports of computer and cybercrimes, the National Computer and Cybercrimes Coordination Committee is responsible for advising the Government on security-related aspects on blockchain technology matters, advising the National Security Council on computer and cybercrimes, co-ordinating national security organs in matters relating to computer and cybercrimes, co-ordination, collection and analysis of cyber threats and response to cyber Incidents that threaten cyberspace

belonging to Kenya and establishing codes of cybersecurity practice and standards of performance for implementation by owners of critical national information infrastructure.

It reports to the Cabinet Secretary responsible for matters relating to internal security and regulates its own procedure.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Any person who fails to report a cyber threat is liable upon conviction of a fine not exceeding Kshs. 200,000.00 or imprisonment for a term not exceeding two years or both.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There are no examples of such enforcement action in Kenya.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Answer not available at the time of print.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

In the financial services sector, the Central Bank of Kenya, which is the regulator of banks, financial institutions and mortgage finance companies, has formulated a Guidance Note on Cyber Security applicable to all institutions licensed under the Banking Act, Chapter 488 of the Laws of Kenya. This Guidance Note sets the minimum standards that institutions must comply with as part of their regulatory obligations and is supplemental to the legislation, regulations and guidelines already in place. It specifically provides for the additional responsibilities of the Board of Directors in relation to cyber risk, senior management responsibility to implement the institution's business strategy, risk appetite and threats, the introduction of the role of the Chief Information Security Officer (CISO), regular independent assessment and testing at least once a year, mitigating the risks of outsourcing services such as cloud providers and providing IT security awareness training programmes for all employees.

The Guidance Note also provides additional reporting requirements for institutions within 24 hours of Incidents that could have a significant adverse impact on the institution's ability to provide adequate services to its customers.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Computer Misuse and Cybercrimes Act contains requirements that are specific to organisations in the financial services sector as well as the telecommunications sector.

For instance, electronic mail or processes through which money or information is being conveyed must not be intercepted or destroyed and electronic messages must be directed to the rightful recipient.

Various acts, such as sending electronic messages which materially misrepresent any fact upon which reliance by another person will cause that person to suffer any damage or loss, as well manipulating a computer or other electronic payment device with the intent to underpay or overpay, are prohibited by the Act.

The Act further prohibits a person authorised to use a computer or other electronic device for financial transactions, issuance of electronic instructions as they relate to sending of electronic debit and credit messages or confirmation of electronic fund transfer from issuing false electronic instructions.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The Principal Officer of a body corporate is required to exercise all reasonable care, skill and diligence when carrying out their duties to prevent the commission of an Incident or any cyber-related crime. In addition to the body corporate being found liable for any offence in the nature of a cybercrime, the Principal Officer or anyone acting in a similar capacity will also be deemed to have committed the offence unless they prove that they exercised their fiduciary duty of care.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Guidance Note on Cybersecurity issued by the Central Bank of Kenya makes all the above recommendations the minimum requirements that institutions licensed under the Banking Act should build upon in the development and implementation of strategies, policies and procedures aimed at mitigating cyber risk.

As part of their cybersecurity policies, organisations have established a unique framework to prevent and indeed mitigate cyber-related risks, which include organisational risk assessment, cybersecurity Incident management, organisation-wide information security awareness and training and regular audits and assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The reporting requirements of any operator of a computer system, whether public or private, only require the entity to disclose information about the breach and knowledge on how the breach occurred, an estimate of the number of people affected, an assessment of the risk of harm to the affected individuals and an explanation of any circumstances that would delay or prevent the affected persons from

being informed of the breach. Service providers, whether public or private institutions, that provide users of its services the means to communicate by use of a computer system or any other entity that processes or stores computer data on behalf of that entity or its users shall not be liable for the disclosure of any data that the service provider discloses to the extent required by the Act.

Listing authorities will specify their disclosure requirements. The contents of a company's annual report will be governed by its articles of association and any other recommendations of the Board. In regulated sectors, however, such as companies in the insurance or banking sector, the regulatory body may specify certain information to be disclosed in the company's annual report.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

This is not applicable in Kenya.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Service providers are liable to both criminal and civil liability if it is established that the service provider had actual notice, actual knowledge, or wilful and malicious intent, and not merely through omission or failure to act, had thereby facilitated, aided or abetted the use by any person of any computer system controlled or managed by the service provider in connection with the contravention of cybersecurity-related laws.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There are no examples of such cases in Kenya.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A potential liability in tort may arise if a complainant is able to demonstrate that an act was committed intentionally against another person with the aim of causing harm or where the offender fails to demonstrate the kind of care a prudent person would take in the same situation and an injury results from any action or inaction.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber Liability Insurance is among the most recent insurance policies available to small and medium-size enterprises as well as large corporations. The policy varies from one insurance provider to another but will typically protect businesses from internet-based risks by mitigating losses relating to damage or loss of information from information technology infrastructure and activities.

As data continues to assert itself as an organisation's most valuable asset, many firms are taking out these types of policies to mitigate the vulnerability of this asset.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Whereas the Insurance Act provides for the framework of insurance policies, no limitations are provided as the risks an insurer can take or mitigate with respect to Cyber Liability Insurance. The insurance policy will vary among the various providers. A first party insurance policy, for instance, will typically cover damage to digital assets, business interruptions, cyber extortion through ransomware and reputational harm, whereas a third-party insurance policy will typically cover liability of cost of forensic investigations, customer notifications, legal defence and regulatory fines.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The law recognises the importance of developing a framework for training employees on the prevention, detection and mitigation of computer and cybercrimes and matters connected thereto. It is also important that cybersecurity awareness and information be provided to customers, clients, suppliers, partners and outsourced service providers.

Whereas the reporting requirements under the Act refer to reporting to the Committee after the occurrence of an Incident, employees owe their employers a reasonable duty of care in the performance of their duties and this would include reporting a potential threat or a security flaw likely to lead to the interception of company data.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The Kenya Access to Information Act, No. 31 of 2016, protects persons making disclosure of information which the person obtained in confidence in the course of employment; for example, if the disclosure is of public interest. Such disclosure may include information on violations of the law.

In the event that there exists any statutory prohibition or restriction on the disclosure of information, it shall be a defence to show that in the circumstances the disclosure was in the public interest and where the offence is alleged to have been committed by a public officer or Government contractor.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The investigatory powers and procedures with respect to cybercrimes and other criminal offences committed by means of a computer system are exercisable by a police officer, an officer in a law enforcement agency or a cybersecurity expert designated by the Cabinet Secretary responsible for matters relating to national security.

Where any of the aforementioned persons has reasonable grounds to believe that a specified computer system or data is reasonably required for the purpose of criminal investigation or has been acquired by a person as a result of the commission of an offence, the authorised person may apply to court for the issuance of a warrant to enter any premises to search and seize such data.

An authorised person may also apply to court for a production order where they have reasonable ground to believe that specified data are in the control of a person or are in the possession of a service provider.

Where there is risk or vulnerability that data may be modified, lost, destroyed or rendered inaccessible, a police officer or any other authorised person has the power to serve a notice on the person who is in possession or control of the computer system requiring the person to undertake expeditious preservation of such data and disclose such data to identify the service provider and that path through which the communication was transmitted.

Subject to making an application to the court and being awarded the relevant order, authorised persons may also collect real-time traffic data, compel a service provider to record data or to co-operate and assist the competent authorities in the collection or recording of data.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Organisations are not required to implement backdoor systems for law enforcement authorities. Authorised persons must adhere to the provisions of the law with respect to accessing any computer system or data and will procure a court order where applicable to access any such system or information.

Note

* The constitutionality of the Computer Misuse and Cybercrimes Act, No. 5 of 2018, has currently been challenged at the Constitution and Human Rights Division of the Kenyan High Court and certain provisions therein have been suspended.

The Act has only recently come into force, and, as of the time of writing, no proceedings have yet been determined under this law.

Hazel Okoth is an Associate at the Head Office in Nairobi and specialises in Commercial, Trade and Intellectual Property matters at the Firm. She holds a degree from the University of Nairobi and a Postgraduate Diploma from the Kenya School of Law. She also holds a Higher Diploma from the Institute of Human Resource Management and is a member of the Project Management Institute as well as the Anti-Counterfeiting Committee of the International Trademark Association (INTA). Hazel has been a delegate and has spoken on various trade-related aspects at the Kenya Trade Week organised by the Ministry of Trade.

In addition to her knowledge on cybersecurity, she has advised on the protection of intellectual property rights in various jurisdictions and undertakes due diligence, investigations and drafts agreements relating to confidentiality, non-solicitation, licences and assignments.

Gikera & Vadgama Advocates
56 Muthithi Road
Behind TRV Office Plaza
Westlands, P.O. Box 720-00621
Nairobi
Kenya

Tel: +254 721 112 167
Email: hokoth@gvalawfirm.com
URL: www.gvalawfirm.com

Stella Ojango is an Advocate of the High Court of Kenya, with over six years' experience as a legal practitioner and is a Partner with the Firm. Stella holds a Bachelor of Laws degree from Moi University, Kenya, and a Postgraduate Diploma in Law from Kenya School of Law. She is currently undertaking her Master's degree in Environmental Law at the University of Nairobi.

Stella has a distinguished track record of delivering valuable advice on real estate projects, from property acquisition, to obtaining the requisite approvals, securing development financing, preparing the requisite contract documents, registration and handover of developments. She is adept at advising institutions on risk management, corporate governance and legal compliance. She has expertise in legislative drafting, intellectual property and cybersecurity law, where she has advised leading corporate institutions on legal measures to be implemented to secure their cyber environment.

Gikera & Vadgama Advocates
56 Muthithi Road
Behind TRV Office Plaza
Westlands, P.O. Box 720-00621
Nairobi
Kenya

Tel: +254 723 755 243
Email: sojango@gvalawfirm.com
URL: www.gvalawfirm.com

Korea


Hwan Kyoung Ko


Kyung Min Son

Lee & Ko

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Under the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "Network Act"), any person who infiltrates another's information communication network ("ICN") without authorised access or beyond the scope of authorised access is subject to imprisonment for not more than five years or a penalty of not more than KRW 50 million.

Similarly, under the Electronic Financial Transactions Act (the "EFTA"), any person who accesses an electronic financial system without authorisation is subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Denial-of-service attacks
Under the Network Act, any person who causes disruption of an ICN by intentionally disturbing network operations with large volumes of signal/data or superfluous requests is subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

Also, under the EFTA, any attacks on electronic financial systems using programs such as a computer virus, logic bomb or email bomb with the intention of destroying data on, or disrupting the operation of, electronic financial systems is subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Phishing
Under the Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss (the "Special Act on Financial Fraud") any person who causes other persons to input data or instructions into computers or other information processing units, or inputs data or instructions into computers or other information processing units by using other persons' data he or she acquires, for the purpose of telecommunications-based financial fraud, is subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Under the Network Act, any person who transmits or distributes malware that can damage, destroy, alter, falsify or disrupt the operation of ICN systems, data or programs, without a justifiable cause, is subject to imprisonment for not more than seven years or a penalty of not more than KRW 70 million.

Moreover, under the EFTA, any person who installs programs, such as a computer virus, logic bomb, or email bomb, for the purpose of destroying data of electronic financial infrastructure or obstructing the operation of electronic financial infrastructure, is subject to imprisonment for not more than 10 years or a penalty of not more than KRW 100 million.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Under the Network Act, any person who mutilates, destroys, alters, or forges an information and communications system, data, program or similar without a justifiable grounds, or conveys or spreads a program that is likely to interrupt the operation of such system, data, program or similar, is subject to imprisonment for not more than seven years or a penalty of not more than KRW 70 million.

Identity theft or identity fraud (e.g. in connection with access devices)
Under the EFTA, a person who forges or alters a means of access (i.e., means or information which is used to issue a transaction request in electronic financial transactions or to secure the authenticity and accuracy of users and the details of such transaction) is subject to imprisonment of not more than seven years or a penalty of not more than KRW 50 million. Moreover, any person who transfers or takes over a means of access, or borrows or lends a means of access in return for receipt, demand or promise of any compensation, is subject to imprisonment of not more than three years or a penalty of not more than KRW 20 million.

Under the Digital Signature Act ("DSA"), any person who steals or discloses another person's digital signature creating key (i.e., a sequence of bits used to affix a digital signature to an electronic message), or has an authorised certificate issued in the name of another person or supports such issuance, is subject to imprisonment of not more than three years or a penalty of not more than KRW 30 million.

Moreover, under the Network Act and the Personal Information Protection Act ("PIPA"), anyone who collects another person's information or induces the provision of another person's information through the ICN by deceptive means, or acquires personal information or obtains the consent for processing of personal information through an illegitimate means or method, is subject to imprisonment for not more than three years or a penalty of not more than KRW 30 million.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Under the Unfair Competition Prevention and Trade Secret Protection Act, any person who acquires, uses, or leaks to any third

party trade secrets for the purpose of making an improper profit or causing damage to a person who possesses trade secrets, is subject to imprisonment for not more than five years or a penalty of not more than KRW 50 million. If such act is considered a breach of fiduciary duty under the Criminal Act, the person is subject to imprisonment for not more than 10 years or a penalty of not less than KRW 30 million. Moreover, if an electronic theft implicates any copyright infringement, such act may result in imprisonment for not more than five years or a penalty of not more than KRW 50 million.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Under the Network act, any person who mutilates another person's information processed, stored or transmitted through an ICN, or infringes, misappropriates or divulges another person's secret, is subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

Failure by an organisation to implement cybersecurity measures

Under the Network Act, information communications service providers ("ICSPs") must, when managing personal information of the data subject (i.e., the owner of the personal information), implement technical and managerial measures to prevent loss, theft, leakage, forgery or alteration of or damage to personal information (collectively, "leakage") and secure the safety of personal information. Failure to do so will be subject to a penalty of not more than KRW 30 million. If any leakage of personal information occurs due to the provider's failure to implement technical and administrative measures, such failure is subject to a penalty of not more than 3% of the sales revenue related to the violation, and imprisonment of not more than two years or a penalty of not more than KRW 20 million.

Moreover, under the EFTA, any financial company, electronic financial business or subsidiary electronic financial business that fails to comply with the standards determined by the Financial Services Commission ("FSC"), which is provided to ensure security and reliability of electronic financial transactions, is subject to a penalty of not more than KRW 50 million.

1.2 Do any of the above-mentioned offences have extraterritorial application?

There is no specific provision in the Network Act or PIPA that stipulates or implicates extraterritorial application of the above-mentioned offences. However, if the information collected and processed outside Korea is that of Korean users, the Korean regulatory authority may find that the Network Act or the PIPA is applicable to such case and impose necessary administrative fines or sanctions under the Network Act or the PIPA. Moreover, the Korean Criminal Act provides that the Act generally applies to aliens who commit crimes, including those provided by other Acts and subordinate statutes, against the Republic of Korea or its nationals outside the territory of the Republic of Korea. Moreover, the EFTA stipulates that, in principle, the Act applies to foreigners or foreign corporations.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

With respect to criminal prosecution of personal information leakage Incidents, the responsible party may be discharged from liability if the requisite safeguard measures (i.e., technical and managerial measures) under the Network Act have been properly implemented.

If the responsible party voluntarily reports such leakage Incident, the Korea Communications Commission ("KCC") may take it into account as a mitigating factor and reduce the amount of penalty to be imposed against the responsible party.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Under the Act on the Protection of Information and Communications Infrastructure (the "PICIA"), any person who disturbs, paralyses or destroys critical ICN infrastructure facilities such as electronic control or managerial systems related to national security, government administration, military defence, policing, finance, telecommunications, transportation and energy is subject to imprisonment for not more than 10 years or a penalty of not more than KRW 100 million.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

In Korea, laws applicable to cybersecurity include: the Network Act; Protection of Communication Secret Act ("PCSA"); PICIA; Electronic Government Act ("EGA"); Act on Establishment of Infrastructure for Informatization of National Defence and Management of Informational Resources for National Defence; EFTA; Credit Information Use and Protection Act (the "Credit Information Act"); Act on the Protection, Use, etc. of Location Information; Act on Prevention of Divulgence and protection of Industrial Technology; PIPA; Act on Prevention of Divulgence and Protection of Industrial Technology; and Special Act on Financial Fraud.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Under the PICIA, the head of the organisation managing the critical ICN infrastructure facilities has an obligation to establish and implement managerial measures, including physical and technical measures (such as prevention, backup, recovery, etc.) to safely protect the facilities and data managed by the organisation.

Under the Network Act, companies that operate clustered information and communications facilities (i.e., business operators who operate and manage clustered information and communications facilities to render information and communications services on behalf of another person (e.g., Internet Data Centre)) are required to take protective measures to stably operate the information and communications facilities.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the "Standards of Technical and Managerial Safeguards for Personal Information" which have been adopted Notice pursuant to the Network Act, ICSPs are required to install and operate systems equipped with the following functions to prevent illegal access and intrusion Incidents via ICNs:

1. functions restricting unauthorised access to the Personal Data Processing System ("PDPS") by limiting access authority by internet protocol ("IP") address etc.; and
2. detect any illegal attempts to acquire personal data by analysing the IP addresses, etc. that accessed the PDPS.

Moreover, under the Network Act, if an intrusion Incident occurs (e.g., intrusion of an ICN or any other related information systems by using the means of hacking, a computer virus, logic bomb, email bomb, denial of service, high-powered electromagnetic wave, etc.), the ICSPs are required to analyse the causes of any intrusion Incidents and keep damage from intrusion at bay.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

It is unlikely that conflict of law issues may arise in relation to the requirements identified in question 2.3 above. It should be noted, however, that the PCSA provides that interfering with transmission and reception of the telecommunications without the consent of the party concerned is a type of "wiretapping" under the Act, and that no person is allowed to wiretap any telecommunications without recourse to the PCSA, the Criminal Procedure Act or the Military Court Act.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Network Act, all ICSPs or Collective ICN Facility Operators must report any "infiltration Incidents" to the Minister of Science and ICT or Korea Internet and Security Agency ("KISA").

In addition, all ICSPs (and providers of similar services) must report any loss, theft, or leakage of personal information, including (i) the items of personal information lost, stolen or leaked, (ii) the time of the occurrence, (iii) actions that can be taken by the data subjects, (iv) protective response measures taken by the personal information service provider, and (v) contact information of the department to which the data subject can make inquiries, to the KCC or KISA within 24 hours since the provider becomes aware of such Incident. The provider may report the Incident after the 24-hour period, only if the provider has a justifiable cause, in which case the provider must explain such cause to the KCC.

In addition, the EFTA requires that if an Incident, such as disturbance or paralysis of an electronic financial infrastructure facility, occurs due to an electronic infringement, the relevant financial company and electronic financial business must, without delay, inform the Incident to the FSC.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

It is not prohibited by law to voluntarily share information relating to Incidents or potential Incidents when such information is not strictly required to be reported. However, the Network Act provides that submission of communication confirmation data (e.g., Internet log data, connection point tracking data) that is made pursuant to the PCSA must satisfy the requirements set forth in the PCSA (e.g., permission of a court).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, under the Network Act, any ICSP who becomes aware of a personal information Incident as described in question 2.5 must notify the data subject of the leaked information, without delay, including the following: (i) items of personal information affected (e.g., leaked); (ii) the timing and circumstances of the leakage; (iii) the actions that can be taken by the data subject to minimise any damages resulting from the Incident; (iv) the protective response measures taken by the personal information service provider; and (v) the name and contact information of the department to which the data subject can make inquires or file a report.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The response to questions 2.5 to 2.7 do not differ, except for point (b) where submission of IP addresses, which are communication confirmation data as explained in question 2.6, must be made in accordance with the provisions set forth in the PCSA.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Ministry of Science and ICT, the Ministry of the Interior and Safety, the Korea Communications Commission, Korea Internet and Security Agency, and the Financial Services Commission.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

A failure to comply with the requirements specified in questions 2.3 to 2.8 may result in a monetary fine imposed by relevant regulatory authorities.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In addition to a monetary fine, the regulatory authorities may require submission of any related articles and documents or enter the place of business of the person concerned to inspect account books and other documents. The regulatory authorities may also order the ICSP to take corrective measures as may be necessary to halt or correct the violation or announce to the public the fact that the provider has received the order to take such corrective measures.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
In Korea, there is no legislation or regulation prohibiting the use of beacons to detect and deflect Incidents in the organisations' networks.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
In Korea, there is no legislation or regulation prohibiting the use of honeypots to detect and deflect Incidents in the organisations' networks.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
In Korea, there is no legislation or regulation prohibiting the use of sinkholes to detect and deflect Incidents in the organisations' networks.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across business sectors because different laws apply depending on the business sector. For example, in the financial sector, the Credit Information Act requires credit information companies to implement certain statutorily prescribed technical, physical, and managerial security measures, including security measures for the use of cloud services and some unique regulations such as network separation to prevent a third party's unlawful access to the company's credit information computer system. With respect to the information communications sector, the Network Act stipulates specific technical and managerial security measures that ICSPs are required to implement in order to prevent the leakage of personal information. As such, when it comes to Governance, Risk Management, Compliance ("GRC") matters, practices vary depending on the industry. In particular, stricter audit and reporting requirements would apply to companies in the financial sector.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) In the financial sector, the EFTA sets forth the standards for ensuring safety with respect to the facilities, electronic apparatus and human resources, which must be implemented by financial companies, electronic financial business entities and subsidiary electronic financial business entities to ensure safety and reliability of the electronic financial transactions.
(b) With respect to the telecommunications sector, the Network Act requires that the following types of ICSPs must obtain a certification for their information protection management system: (i) common telecommunications business operators providing ICN services in Seoul Special Metropolitan City and any other Metropolitan Cities; (ii) companies that operate clustered information and communications facilities; and (iii) companies whose revenue generated in the sector of information and communications services in the previous year is not less than 10 billion won, or whose average number of daily users over the past three months is not less than one million.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The Network Act requires that the CISO must be designated from the company's director-level employees (unless the ICSP or the like is a small business). If the CISO has reported issues relating to a potential Incident to the board of directors or representative director, and the directors have failed to properly respond to prevent the Incident occurring, such failure may amount to a breach of directors' duties.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) Under the amended version of the Network Act, in principle, all ICSPs (other than small business enterprises) must designate a director-level CISO and report such fact to the Ministry of Science and ICT. The CISO of a company that meets certain thresholds in terms of their assets or number of employees (e.g., the company's total assets at the end of the immediately preceding business year was at least KRW 5 trillion) may not perform any duties other than that of the CISO as prescribed by law. Any financial company or electronic financial business must also appoint a CISO, and the CISO may not perform any duties other than that of the CISO if the financial company or electronic financial business entity meets certain thresholds in terms of their assets or number of employees.

(b) Any personal information processor that processes personal information of 10,000 data subjects or more must establish a manual which provides information regarding the measures to be implemented in response to personal information leakage Incidents.

(c)/(d) Under the EFTA, financial companies and electronic financial business must analyse and assess the vulnerability of electronic financial infrastructure, including the assessment on the information technology sector, at least once each business year. Moreover, under the PICIA, the head of the management organisation of the critical information and communications infrastructure must analyse and evaluate the vulnerabilities of the infrastructure every year.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the Network Act, the Minister of Science and ICT may order the ICSPs and the Collective ICN Facility Operators to do the following, if he or she finds that it is necessary to analyse the cause of the infiltration Incident:

(i) retain relevant material such as records of access to the ICN;
(ii) submit the relevant material to the infiltration Incident; and
(iii) allow physical access to the business site to investigate the cause of the Incident.

Moreover, the providers of critical information communications services and the Collective ICN Facility Operators must submit information regarding any infiltration Incident, such as statistics by type of intrusion cases, statistics of traffic of the relevant ICNs, and statistics of use by access channel, to the Ministry of Science and ICT and KISA.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Pursuant to the Network Act, the Minister of Science and ICT may issue a public notice of guidelines for protective measures for information and may recommend that ICSPs observe the guidelines. The Minister of Science and ICT may also recommend that anyone who intends to carry out an information and communications service business or telecommunications business of a certain size requiring a licence, permit, registration, or report to take protective measures in accordance with the preliminary examination standards for data protection (i.e., the "Public Notice on Preliminary Examination of Data Protection").

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the event that an Incident occurs due to the personal information processor's violation of the PIPA, the data subject may claim damages against the personal information processor. In this case, the personal information processor will be liable for damages unless it can prove that there was no wilful misconduct or negligence of the processor that caused the Incident. If the data subject incurs any damages caused by the Incident due to the personal information processor's wilful misconduct or gross negligence, the court may award up to treble damages. Also, the data subject may seek statutory damages up to KRW 3 million, if the Incident was caused by wilful misconduct or negligence of the personal information processor.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

In 2014, there was a personal information leakage Incident of over 100 million items of personal information stored by one of the major card companies in Korea being leaked. The victims of the leakage brought a claim against the company and the court awarded damages in the amount of KRW 10,000 to each of the plaintiffs for the leakage Incident. Moreover, in recent years, the amount of fines imposed against companies involved in a leakage Incident increased substantially, as it is shown in the case where an internet shopping site was required to pay an administrative fine of KRW 4.5 billion (approx. USD 3.8 million) for a leakage Incident.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The personal information processor may be found liable for a tort under Korean Civil Act, if the plaintiff proves that (i) there was a violation of relevant data protection laws by the processor of the personal information, (ii) the data subject has incurred damages due to the Incident, (iii) there is a causal relationship between the damage and the violation, and (iv) there has been wilful misconduct or negligence by the processor.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Under the Network Act, ICSPs of a certain size must purchase liability insurance policy, join a mutual aid programme or accumulate reserves for compensation of damages to their users, if any. Moreover, under the Credit Information Act, financial companies and credit information companies must also take measures necessary to fulfil liability to compensate damage by purchasing insurance, joining a mutual aid programme, or accumulating reserves.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No. As a reference matter, among the insurances mentioned in question 6.1 above, the insurance required under the Network Act is intended to ensure the ICSP's compensation of damages incurred by the user as a result of the ICSP's wilful misconduct or negligence amounting to a violation of the data protection/privacy provisions under the Network Act.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) From the outset, an ICSP is required to implement technical/managerial security measures in order to ensure the security of its users' personal information. For example, access to the ICSP's personal information processing system must be limited to only those personal information managers necessary for providing services to users, and records on the grant, change, or termination of a personal information manager's access rights must be retained for at least five years. In relation to this, the ICSP must check/inspect the access records of the personal information processing system maintained by the personal information managers at least once a month, and retain the records for at least six months (one year under the PIPA).

(b) There are no statutory requirements for employees to report Incidents or potential Incidents to their employer. However, based on the Korean regulators' guideline titled "Manual for Responding to Personal Information Leakage Incidents", all employees are required to immediately report any Incidents or potential Incidents to the responsible data protection officer via email, phone or the like.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No. Rather, any person who believes that an act detrimental to the public interest has been, or is likely to be, committed may file a public interest report. An "act detrimental to the public interest" includes an act that is subject to penalties or administrative sanctions under the PIPA, Network Act, or Credit Information Act. Therefore, the reporting of an Incident by an employee is protected under the Protection of Public Interest Reporters Act.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The following authorities have investigatory powers of law enforcement: National Intelligence Service; National Police Agency Cyber Bureau; Forensic Science Investigation Department of the Supreme Prosecutors' Office; Financial Supervisory Service; and KISA.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there is no legislation or regulation in Korea that requires organisations to implement backdoors in the IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys.

Hwan Kyoung Ko is a partner in the Technology, Media & Telecommunications / Data Protection and Cybersecurity and Fintech Practice Group. He is regarded as a leading expert in the telecommunication, data protection and cybersecurity and Fintech regulation field and has been recognised as a leading lawyer of the year in the TMT practice area by *Legal Times* in 2016. He has advised numerous BigTech/IT companies and government agencies, on data protection and cybersecurity-related issues. Mr. Ko has also been involved in efforts to promote the Big Data industry in Korea, as witnessed by his participation in a recent Hackathon event hosted by the Presidential Committee on the Fourth Industrial Revolution.
Mr. Ko is a recipient of the 2019 Presidential Citation (for active involvement in the promotion of legislation to drive the Data Economy), the 2016 Minister of the Interior and Safety's Award (in the data protection sector) and the 2014 KISA President's Award for Personal Data Protection.
Mr. Ko holds a B.A. from Korea University and an LL.M. from Georgetown University Law Center. He is admitted to the New York and Korean Bars.

Lee & Ko
Hanjin Building 63
Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4000
Fax: +82 2 772 4001/2
Email: hwankyoung.ko@leeko.com
URL: www.leeko.com

Kyung Min Son is a partner in the Technology, Media and Telecommunications practice Group at Lee & Ko. He has advised various telecommunications and IT companies, with a focus on various issues in all TMT areas, including mobile and regulatory issues in internet services, such as issues on privacy, internet contents, and internet advertisements.
He also has expertise in the areas of Data Privacy & Cybersecurity, Fintech, where he represents various domestic and foreign companies.
Prior to joining Lee & Ko, Mr. Son served as a judge advocate officer for the Korean Navy.
Mr. Son received his LL.B. from Seoul National University and his LL.M. from the University of Southern California. He is admitted to the Seoul Bar.

Lee & Ko
Hanjin Building 63
Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4918
Fax: +82 2 772 4001/2
Email: kyungmin.son@leeko.com
URL: www.leeko.com

Lee & Ko's evolution as the premier law firm in Korea parallels in many ways the solid economic development of the country for more than 40 years. Our firm is one of the top law firms in Korea that is recognised for its expertise in over 30 specialised practice areas, and consistently acclaimed over the years as one of the leading firms in Asia by internationally respected legal publications and league tables. Lee & Ko has a global client base that includes multinational corporations in many different industries.
In particular, the firm's DPC/TMT team (Data Privacy & Cybersecurity/ Technology, Media & Telecommunications) has extensive experience, knowledge, and expertise in a wide range of cases involving, among others, security breaches, hacking Incidents and DPC/TMT-related regulatory issues, transactional matters and litigations. The team is known as one of the top experts in the field with unrivalled knowledge and knowhow in Korea.

www.leeko.com

Kosovo

Renata Leka

Delvina Nallbani

Boga & Associates

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Law No. 03/L-166 "On prevention and fight against cyber crime" ("Cyber Crime Law") provides for criminal offences related to the misuse of computer systems and computer data, although it does not provide a literal denomination of the criminal offences listed below.

Subject to the Cyber Crime Law, unauthorised access to computer systems constitutes a criminal offence, punishable by imprisonment for up to three years. Unauthorised actions are classified actions performed by a person: (i) who is not authorised by law or contract; (ii) who exceeds the limits of his/her authorisation; and/or (iii) has no permit and is not competent and qualified to use, administer or control a computer system or conduct scientific research on a computer system.

If such an offence is committed for the purpose of obtaining computer data or violates computer security measures, the penalties provided by law are higher and such offences are punishable by imprisonment for up to four years and five years, respectively.

In addition, the Criminal Code (Law No. 06/L-074) provides for the criminal offence of intrusion into computer systems. In this regard, whoever, without authorisation and in order to gain an unlawful material benefit for himself or another person or to cause damage to another person, alters, publishes, suppresses or destroys computer data or programs, or in any other way enters another's computer system, is punished by a fine and up to three years of imprisonment. If the offence results in a material gain exceeding 10,000 Euros or material damage exceeding 10,000 Euros, the perpetrator shall be punished by a fine and by imprisonment of up to five years.

Denial-of-service attacks
The serious hindrance of the functioning of computer systems, performed by entering information, transferring, changing, removing or destroying computer data or unauthorised limiting of access to such data, is stipulated as a criminal offence pursuant to the Cyber Crime Law, and the perpetrator is liable to imprisonment for up to three years. Such offence shall be punished by imprisonment for up to five years if committed by a member of a criminal organisation.

Phishing
We have not identified a criminal offence provided by the Cyber Crime Law or other applicable laws that would represent phishing. However, each criminal activity that aims to misuse computer systems or computer data should be considered individually to establish whether it constitutes a criminal offence provided for by the Cyber Crime Law or any other applicable law.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
We have not identified a criminal offence provided by the Cyber Crime Law or other applicable laws that would constitute infection of IT systems with malware. However, each criminal activity that aims to misuse computer systems or computer data should be considered individually to establish whether it constitutes some other criminal offence provided for by the Cyber Crime Law or any other applicable law.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Pursuant to the Cyber Crime Law, the illegal production, sale, import, distribution or making available, in any form, of any equipment or computer program designed and adapted for the purpose of committing any criminal offence is punishable by imprisonment from one to four years.

Further, the illegal production, sale, import, distribution or making available, in any form, of passwords, access codes or other computer information that would allow full or partial access to a computer system for the purpose of committing any criminal offence shall be punishable by imprisonment from one to five years.

In addition, the illegal possession of equipment, computer programs, passwords, access codes or computer information for the purpose of committing any criminal offence is punishable by imprisonment from one to six years.

An attempt to commit this criminal offence is also punishable by imprisonment, ranging from three months to one year.

Identity theft or identity fraud (e.g. in connection with access devices)
We have not identified any criminal offence provided by the Cyber Crime Law or other applicable laws that would constitute identity theft or identity fraud. However, as mentioned above, such criminal activities should be assessed individually.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Pursuant to the Criminal Code (Law No. 06/L-074), any act of circumvention of any effective technological protection measure or any act of removal or alteration of electronic rights management information, as provided for by the Law "On copyright and related rights", shall be punishable by imprisonment for up to three years.

Subject to the Law "On copyright and related rights" (Law No. 04/L-065 as amended), violation of the rights protected by this law

would be considered if a person processes, imports for distribution, sells, lends, advertises for sale or lease or keeps for commercial technological purposes a computer program, or carries out services without authorisation, and if such actions: (i) are advertised or traded especially for the purpose of avoiding effective technological measures; (ii) have evident commercial purpose or have been used solely for avoiding effective technological measures; and (iii) are designed, produced, adapted or processed primarily with the purpose of avoiding effective technological measures. An effective technological measure is considered to be any technology, computer program or other means intended to prevent or remove a violation of a protected right.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

In addition to the criminal offences listed above, the Cyber Crime Law also provides for the following criminal offences related to computer systems and computer data: the unauthorised entry of data; change or deletion of computer data; and the unauthorised limitation of access to such a data resulting in inauthentic data.

Also, causing a loss in assets to another person by entering information, changing or deleting computer data by means of access limitation to such data, or any other interference into the functioning of a computer system with the purpose of ensuring economic benefits for himself or for someone else, shall be punishable with up to 10 years of imprisonment.

Failure by an organisation to implement cybersecurity measures

We have not identified such a criminal offence provided by the applicable legislation.

1.2 Do any of the above-mentioned offences have extraterritorial application?

In addition to the criminal offences committed within the Kosovo territory, the abovementioned laws that stipulate criminal offences will also apply to persons who have committed criminal offences outside the territory of Kosovo, if provided for by an international agreement by which Kosovo is bound.

Criminal legislation of the Republic of Kosovo shall also apply to any Kosovo citizen or a foreigner who commits a criminal offence outside the territory of the Republic of Kosovo if the criminal offence is also punishable in the country where the offence was committed. In case of foreigners, these provisions shall apply if the foreigner is found in the territory of Kosovo or has been transferred to Kosovo.

However, the criminal proceedings against a Kosovo citizen or a foreigner for criminal offences committed outside Kosovo territory will not be undertaken if the perpetrator has fully served the punishment imposed in another jurisdiction, has been acquitted by a final judgment and/or released from punishment or punishment has become statute-barred and in cases where criminal proceedings may only be initiated upon the request of the injured party and such a request has not been filed.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Subject to article 8 of the Cyber Crime Law, for a category of computer systems to which access is restricted or completely forbidden, the owners and administrators of such a computer system are obliged to clearly and automatically warn the user of this computer system, and to provide him/her with information, as well as conditions of use, or forbiddance to use this computer system and legal consequences for unauthorised access to this computer system. Failure to comply with such an obligation is considered a misdemeanour and the perpetrator is punished with a fine ranging from 500 to 5,000 Euros.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The Criminal Code provides that issuing blank or false cheques and the misuse of bank or credit cards constitutes a criminal offence. Such an offence is defined as an act committed for the purpose of gaining unlawful material benefit for the perpetrator or for another person, by issuing or placing into circulation cheques which the perpetrator knows are not covered by material means. The placing of false cheques or counterfeit credit cards is punished by a fine and imprisonment for up to three years. In relation to prosecution of this criminal offence in a cybersecurity context, there is a case pending before Kosovo courts where the defendant has been prosecuted for violation of the Cyber Crime Law, specifically for the possession or use of passwords, hardware, software or other tools to commit cybercrime.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The Applicable Laws relevant to cybercrime are listed below.

Law No. 03/L-166 "On prevention and fight against cybercrime"; Law No. 06/L-074 "Criminal Code of The Republic Of Kosovo"; Law No. 04/L-094 "On the information society services"; Law No. 04/L-109 "On electronic communications"; Law No. 05/L-030 "On interception of electronic communication"; Law No. 06/L-082 "On the protection of personal data"; Law No. 04/L-149 "On the execution of penal sanctions", as amended; Law No. 04/L-065 "On copyright and related rights" as amended; Law No. 04/L-093 "On banks, microfinance institutions and non-bank financial institutions"; Law No. 04/L-198 "On the trade of strategic goods"; Code No. 03/L-109 "Customs and excise code of Kosovo" as amended; and Law No. 03/L-178 "On classification of information and security clearances".

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Kosovo is not an EU member; however, the Ministry of Internal Affairs has adopted the State Strategy for Cyber Security and the Action Plan for 2016 to 2019, drafted based on European Union practices and policies.

The Kosovo Government has also made the Kosovo Police available as a permanent contact point for international cooperation in the field of cybercrime. In this regard, the Kosovo Police should ensure ongoing international cooperation and assistance in the field of cybercrime, order data retention and confiscation of equipment containing data, as well cooperate with all competent Kosovo authorities while undertaking execution actions.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Cyber Crime Law provides that authorities and public institutions with competence in this area, service providers, non-governmental organisations and civil society representatives should carry out activities and programmes for the prevention of cybercrime and develop policies, practices, measures, procedures and minimum standards for the security of computer systems and should also organise information campaigns on cybercrime and risks for computer system users.

The Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Transport and Communications, the Ministry of Public Services, and the Kosovo Intelligence Services shall develop special training programmes for personnel for the purpose of preventing and fighting cybercrime in accordance with specific competencies.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

We have not identified any provisions that could lead to conflicts of laws issues. However, in certain cases, the provisions of Law No. 05/L-030 "On interception of electronic communications", which govern the procedures and conditions for authorised interception of electronic communications, may come into conflict with the measures for surveillance, detection, prevention or mitigation of an Incident by authorised authorities in the cybercrime area.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no obligation to report information related to Incidents to a special authority in Kosovo. However, the Cyber Crime Law provides that the Ministry of Justice, in cooperation with the Ministry of Internal Affairs, shall continuously maintain and supplement the database on cybercrime.

In principle, in order to report any criminal offence, a criminal complaint may be filed by any person to the police station in the area where the crime was committed or to the competent state prosecutor in writing, by technical means of communication or orally. For practical reasons, criminal offences are typically reported to the police station.

After receiving information of a suspected criminal offence, the police shall investigate whether there is reasonable suspicion that a criminal offence prosecuted *ex officio* has been committed. The police shall investigate a criminal complaint and shall take all the necessary steps (i.e. to locate the perpetrator, to prevent, detect and preserve traces and other evidence, to collect all the information that may be of use in criminal proceedings, etc.). In order to perform these tasks, the police are authorised, under the provisions of the Criminal Procedure Code (Law No. 04/L-123), to gather information from individuals, to take all the necessary steps to establish the identity of the persons, and to interview witnesses or possible suspects, etc.

Based on such collected information, the police draft the criminal complaint and submit it to the competent state prosecutor. The public prosecutor is obliged to act according to the criminal complaint, i.e. to initiate proceedings (file an indictment) or to dismiss the criminal complaint.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

The applicable legislation is silent in this regard.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Subject to the Cyber Crime Law, the prosecutor is obliged to notify in writing, by the end of the investigation, the persons who are under investigation.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The applicable legislation does not address this issue.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The State Prosecutor and the Courts are the institutions responsible for the prosecution and punishment of perpetrators of criminal offences and for the confiscation of property acquired through criminal offences.

Also, listed below are institutions relevant to the cybercrime area:

- The Ministry of Internal Affairs is responsible for the drafting and monitoring of policies and legislation in the field of overall security and cybersecurity.
- The Kosovo Police, as a law enforcement agency, has the primary responsibility in combatting all forms of cybercrime within the Cybercrime Sector and for implementing specific supporting structures. The Kosovo Police also serves as a contact point for international cooperation in the field of cybercrime.
- The Kosovo Security Council Secretariat, as an integral part of the Kosovo Security Council, prepares periodic reports for the Government of the Republic of Kosovo and the Kosovo Security Council dealing with security policy issues.
- The Kosovo Intelligence Agency identifies threats that endanger Kosovo's security, such as the threat to territorial integrity, institutional integrity, constitutional order, stability and economic development, as well as threats to global security to the detriment of Kosovo.
- The National Agency for the Protection of Personal Data ensures that controllers respect their obligations regarding the protection of personal data and that data subjects are informed about their rights and obligations in accordance with the Law "On protection of personal data".
- The Ministry of Justice, the Ministry for the Kosovo Security Force, the Ministry of Economic Development, the Ministry of Foreign Affairs, the Ministry of Finance, as well as the Regulatory Authority of Electronic Data and Postal Communications and the Information Society Agency contribute to cybersecurity in their relevant fields.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There are no penalties provided by the applicable legislation.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

We are not aware of any enforcement actions taken in this area.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The applicable legislation does not specify if these measures are permitted or not. Referring to the prevention, security and information campaigns, "The Cyber Crime Law" provides that authorities and public institutions with competence in this area, service providers, non-governmental organisations and civil society representatives should carry out activities and programmes for the prevention of cybercrime and develop policies, practices, measures, procedures and minimum standards for the security of computer systems and should also organise information campaigns on cybercrime and risks for computer system users.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
The applicable legislation does not specify if these measures are permitted or not.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The applicable legislation does not specify if these measures are permitted or not.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

There is no consolidated practice in the area of cybercrime to make this assessment.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

There are no specific requirements as regards cybersecurity in different organisations. However, as regards the telecommunication sector, there are specific obligations for the purpose of criminal proceedings for entrepreneurs of public electronic communications services and networks based on the Law "On electronic communications" (Law No. 04/L-109). As regards the financial sector, financial institutions in Kosovo are bound by the provisions of the Law "On the prevention of money laundering and combatting financing of terrorism" (Law No. 05/L-096), which provides measures and procedures for detecting and preventing criminal offences of money laundering and combatting terrorist financing.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

We have not identified such circumstances based on the applicable legislation.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no such responsibility provided under the Applicable Laws for companies.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, they are not.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, they are not.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Civil actions that may be brought would be those claiming compensation of damages in virtue of the Law "On obligations relationship" (Law No. 04/L-077). In that case, the culpability of a person that has caused damages in relation to any Incident should be proven.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

From the review of some of the published decisions of the Basic Courts and the Supreme Court adopted during 2017 and 2018, we have not identified any decision adopted in this respect. Based on media reports, there have been several cases of prosecution for possession or use of passwords, software or other tools to commit cybercrime, prosecuted in connection with the criminal offence of abuse of banks and credit cards.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

There are no such liabilities provided under Kosovo law.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Such type of insurance does not exist in practice.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no such regulatory limitations provided by the Applicable Laws.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no such requirements provided by the applicable legislation.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

We have not found any provisions in the Law "On witness protection" (Law No. 04/L-015) that may limit the reporting of Incidents. The law provides for special and urgent measures and procedures for witness protection if there is a serious threat to a person and the person's close relatives and if that person agrees to cooperate closely with the courts or investigatory authorities.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Pursuant to the Criminal Procedure Code (Law No. 04/L-123), the state prosecutor may undertake investigative actions or authorise the police to undertake investigative actions regarding the collection of evidence. In the latter case, the police shall investigate criminal offences and shall take all the steps necessary to locate the perpetrator, to prevent the perpetrator or his/her accomplice from hiding or fleeing, to detect and preserve traces and other evidence of the criminal offence and objects which might serve as evidence, and to collect all the information that may be of use in the criminal proceedings.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements.

Renata Leka is a Partner at Boga & Associates, which she joined in 1998. She is specialised in intellectual property, data protection, and cybersecurity.
Renata is an authorised trademark agent and has ample experience in trademark filing strategy, portfolio management and trademark prosecution, and handles a range of international matters involving IPR issues. She manages anti-piracy and anti-counterfeit programmes regarding violation of copyright in Albania and assists international clients in all aspects of the IPR.
Renata graduated in Law at the University of Tirana in 1996 and also holds Practice Diploma from the College of Law of England and Wales, UK in International Intellectual Property Law (2006) and in Anti-Trust Law (2009).
Renata is fluent in English and Italian.

Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 225 1050
Fax: +383 38 223 153
Email: rleka@bogalaw.com
URL: www.bogalaw.com

Delvina Nallbani is a Senior Manager at Boga & Associates, which she joined in 2012.
She is specialised in intellectual property, data protection and privacy, commercial contracts and cybersecurity.
Delvina has extensive experience in providing legal advice to both domestic and multinational clients on a wide range of corporate, mergers and acquisitions, business and banking matters. She also provides assistance in advising investors on a number of transactions including project finance, mergers and acquisitions, and privatisations.
Delvina graduated in law from the University of Zagreb and is member of the Kosovo Bar Association.
She is fluent in Albanian, Croatian and English.

Boga & Associates
27/5 Nene Tereza Str.
10000 Pristina
Kosovo

Tel: +383 38 223 152
Fax: +383 38 223 153
Email: dnallbani@bogalaw.com
URL: www.bogalaw.com

Boga & Associates, established in 1994, has emerged as one of the premier law firms in Albania and Kosovo, earning a reputation for providing the highest quality of legal, tax and accounting services to its clients. Until May 2007, the firm was a member firm of KPMG International and the Senior Partner/Managing Partner, Mr. Genc Boga, was also the Senior Partner/Managing Partner of KPMG Albania.
The firm's particularity is linked to the multidisciplinary services it provides to its clients, through an uncompromising commitment to excellence. Apart from the widely consolidated legal practice, the firm also offers the highest standards of expertise in tax and accounting services, with keen sensitivity to the rapid changes in the Albanian and Kosovo business environment.
The firm delivers services to leading clients in major industries, banks and financial institutions, as well as to companies engaged in insurance, construction, energy and utilities, entertainment and media, mining, oil and gas, professional services, real estate, technology, telecommunications, tourism, transport, infrastructure and consumer goods.
The firm is continuously ranked as a "top tier firm" by major directories: *Chambers Global*; *Chambers Europe*; *The Legal 500*; and *IFLR 1000*.

www.bogalaw.com

BOGA & ASSOCIATES
LEGAL • TAX • ACCOUNTING

Malaysia

Christopher & Lee Ong

Deepak Pillai

Yong Shih Han

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under section 3 of the Computer Crimes Act 1997 ("**CCA**"), it is an offence if a person knowingly and intentionally accesses a computer without authorisation and causes a computer to perform any function with the intent to secure access to any program or data held in any computer.

A person found guilty of an offence under section 3 is liable to a fine not exceeding RM50,000 or imprisonment not exceeding five years or both.

In *PP v Vishnu Devarajan* [2016] 1 LNS 1066, the accused was charged under section 3 of the CCA for accessing, without authorisation, the servers of a broadcast centre and the server database of a Malaysian radio network company. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

Section 4 of the CCA creates a further offence against persons who commit a hacking offence under section 3 with the intent to: (i) commit an offence involving fraud or dishonesty which causes injury under the Malaysian Penal Code (the main penal statute in Malaysia) (the "**Penal Code**"); or (ii) facilitate the commission of such an offence whether by himself or any other person. A person found guilty under section 4 is liable to a fine not exceeding RM150,000, or imprisonment not exceeding 10 years, or both.

In *Basheer Ahmad Maula Sahul Hameed v PP* [2016] 6 CLJ 422, the two accused persons, who were husband and wife, where the wife worked in a bank, were convicted under section 4(1) of the CCA for using a debit card belonging to an airplane accident victim to withdraw cash from an ATM machine and for transferring money from several other victims' online banking accounts without authorisation.

Denial-of-service attacks

There is no specific provision which provides for denial-of-service attacks. However, under section 233(1)(b) of the Communications and Multimedia Act 1998 ("**CMA**"), a person who continuously, repeatedly or otherwise initiates a communication using any applications services with the intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence, regardless of whether the communication ensued and whether or not the person initiating such communication disclosed their identity.

A person found guilty of an offence under section 233(1)(b) is liable to a fine not exceeding RM50,000, or imprisonment not exceeding one year, or both, and shall also be liable to a further fine of RM1,000 for every day that the offence is continued after conviction.

To date, there have been no reported cases under section 233(1)(b) of the CMA which specifically relate to denial-of-service attacks.

Phishing

There are no specific offences with regard to phishing. However, other statutory provisions may be applicable in tackling phishing offences.

Under section 416 of the Malaysian Penal Code, any person is said to "cheat by personation", if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. The offence of cheating by personation is punishable with imprisonment for a term which may extend to seven years and/or a fine.

To date, there are no reported cases specifically in relation to phishing.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Infection of IT systems with malware is an offence punishable under the CCA. Under section 5 of the CCA, it is an offence for a person to commit any act which he knows will cause unauthorised modification of the contents of any computer.

A person found guilty of an offence under section 5 is liable to a fine not exceeding RM100,000 or imprisonment not exceeding 10 years, or both if the act was committed with the intention of causing injury.

In *PP v Roslan and Anor* [2016] 1 LNS 651, the accused who worked as a Systems Analyst in the IT Department of the Malaysian Hajj Pilgrims Fund Board, was convicted under section 5(1) of the CCA for modifying pilgrims' records in the organisation's database without authorisation.

In *PP v Vishnu Devarajan* [2016] 1 LNS 1066, the accused was charged under section 5 of the CCA for, amongst others, carrying out the following without authorisation: downloading and launching software; running and stopping certain processes on servers; and running certain programs on the database server of a broadcast centre. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

In *Kangaie Agilan Jammany v PP* [2017] 1 LNS 1640, the accused, an employee of AirAsia, a low-cost airline carrier company, was charged under section 5 of the CCA where he used the Air Asia reservation system without authorisation to modify passenger flight schedules, in order to help family members and friends obtain airline tickets at lower rates.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Under section 236 of the CMA, it is an offence for a person to possess or use any counterfeit access devices, unauthorised access devices (e.g. lost, stolen, expired, or obtained with the intention to defraud), any device-making equipment intended to make counterfeit access devices, or any other equipment or device modified or altered or intended to alter or modify such other equipment or device in order to obtain unauthorised access to any network services, etc.

Possession or use of the above is an offence and the offender would be liable to a fine not exceeding RM500,000 or to imprisonment not exceeding five years, or both.

Under section 240 of the CMA, it is an offence to distribute or advertise any communications equipment or device for interception of communication. An offence under this section would render the offender liable to a fine not exceeding RM100,000 or to imprisonment not exceeding two years, or both.

To date, there have been no reported cases either under section 236 or section 240 of the CMA.

Identity theft or identity fraud (e.g. in connection with access devices)

The Penal Code contains provisions on cheating by personation. Although not cyber-specific, section 416 of the Penal Code (as discussed above) may apply to identity theft. Under section 416 of the Penal Code, it is an offence to "cheat by personation", i.e. where a person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such person really is.

To date, while there has been news of individuals committing identity theft or fraud, such cases have, however, usually been tried on the basis of contravening national registration regulations (in relation to impersonating or theft of identification cards). There have been no reported cases for actions on identity theft or identity fraud specifically in the context of cybersecurity or cybercrimes.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Under Malaysian law, the right to bring an action for breach of confidence stems from common law, or pursuant to the contracts of employment, which generally contain confidentiality clauses and as such would not constitute a criminal offence.

Copyright owners have the right to bring an action for copyright infringement either as a civil or criminal offence. Section 41 of the Copyright Act 1987 sets out a range of offences for copyright infringement, which include making for sale or hire, distributing, and exhibiting in public any infringing copy during the subsistence of copyright in a work or performers' right.

In *Chuah Gim Seng & More Again v. SO* [2009] 10 CLJ 65, the appellants were found guilty and convicted for the sale of pirated copy films. The penalty imposed was RM2,000 for the sale of each copy and in default a four-month jail term for failure to pay each charge.

In *PP v. Haw Swee Po* [2011] 5 LNS 23, the accused was tried for possession and use (other than for private and domestic use) of 3,300 copies of seven films in DVD format. The court sentenced the accused to 14 months' imprisonment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Activities which adversely affect or threaten security, confidentiality, integrity or availability of IT systems, infrastructures, etc. are prohibited or regulated under the CMA. For example, it is an offence to: use any apparatus or device with the intent to obtain information regarding the contents, sender or addressee of any communication without an approval by a registered certifying agency (section 231 of the CMA); possess or create a system designed to fraudulently use or obtain any network facilities, network service, applications service or content applications service (section 232(2) of the CMA); intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept, any communications (section 234 of the CMA); and extend, tamper with, adjust, alter, remove, destroy or damage any network facilities or any part thereof (section 235 of the CMA).

A person who is found liable for any of the above offences under CMA may, upon conviction, be held liable to a maximum fine ranging from RM50,000 to RM300,000 or imprisonment not exceeding two to three years, or both.

In relation to personal data, organisations are required to ensure the security of individuals' personal data (section 9 of the Personal Data Protection Act 2010, the "**PDPA**"), and in this regard are required to comply with the minimum security standards prescribed by the Personal Data Protection Standards 2015 (the "**PDP Standards**"). Non-compliance with section 9 of the PDPA may hold the offender liable to a fine not exceeding RM100,000 or imprisonment not exceeding two years, or both, whereas non-compliance with any of the security standards under the PDP Standards may result in the offender being held liable to a fine not exceeding RM250,000 or imprisonment not exceeding two years, or both.

To date, there have been no reported cases prosecuted under any of the abovementioned provisions of the CMA or PDPA.

Failure by an organisation to implement cybersecurity measures

There is currently no legislation which imposes a blanket requirement in respect of implementing cybersecurity measures. The closest is the PDPA, which only applies to organisations involved in commercial transactions and expressly excludes the Government of Malaysia.

Organisations that are involved in processing personal data are required to implement minimum security standards as prescribed by the PDP Standards, or such other standards as prescribed by the Personal Data Protection Commissioner (the "**PDP Commissioner**") from time to time.

Certain sectors are additionally subject to the guidelines requiring the implementation of certain cybersecurity measures, for example:

(a) in the capital market industry, capital market entities are subject to cybersecurity requirements as set out in the *Guidelines on Management of Cyber Risk* issued by the Securities Commission of Malaysia ("**SC**"); and

(b) in the banking and financial sector, banks and financial institutions are subject to the requirements as set out in the *Policy Document on Risk Management in Technology* ("**RMiT**") issued by the Central Bank of Malaysia or Bank Negara Malaysia ("**BNM**").

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes. The CCA, CMA, and to a certain extent, the Penal Code (in relation to terrorism and offences against the state) have extraterritorial application.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

For organisations that are subject to cybersecurity obligations or requirements (e.g. PDPA, sector-specific cybersecurity requirements),

there are no specific actions specified in the statutes or guidelines which might mitigate the penalty which would otherwise be incurred by reason of any breach or non-compliance by the organisation. However, it is reasonable to infer that cooperation with the relevant regulators or enforcement authorities, or active steps taken to mitigate the loss or damage caused by any of the offences, may serve to mitigate the severity of penalty to be imposed by the regulators or enforcement authorities.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

It is generally an offence (even though not specific to cybersecurity) to commit or facilitate terrorism activities, e.g. where there is financing of terrorism, or participation or indication of support to terrorist groups or activities (section 130J of the Penal Code).

In the context of cyberterrorism, sub-section (2)(k) of section 130J specifically provides that "support" to a terrorist group extends to the act of "using social media or any other means to:

(i) advocate for or to promote a terrorist group, support for a terrorist group or the commission of a terrorist act; or
(ii) further or facilitate the activities of a terrorist group".

While Malaysian enforcement authorities have regularly taken steps to block or remove known terrorist websites, there have been no reported cases in respect of cyberterrorism under the abovementioned section 130J(2)(k) of the Penal Code.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import / export controls, among others.

As at the time of writing, there is no single legislation in Malaysia in respect of cybersecurity. In June 2017, the then Malaysian Home Minister, Ahmad Zahid Hamidi, announced that a new cybersecurity bill will be drafted and tabled in Parliament in order to combat cybercrimes, including recruitment and financial sourcing by terrorist groups, money laundering and online gambling. However, the cybersecurity bill has not been tabled in Parliament to date, and therefore it appears that the draft bill has been shelved.

Instead, the National Cyber Security Agency (as the national lead agency under the National Security Council of the Prime Minister's Department for cybersecurity matters, with the objectives of securing and strengthening Malaysia's resilience in facing the threats of cyber attacks) is reported to have been tasked with spearheading a national cybersecurity strategy, including the preparation and implementation of the National Cyber Security Policy and National Cyber Crisis Management Plan.

Notwithstanding the above, the current laws which relate to cybersecurity in Malaysia include:

Communications and Multimedia Act 1998 (CMA)
The CMA provides for and regulates the converging areas of communications and multimedia. In particular, the CMA regulates various activities carried out by licensees (i.e. network facilities providers, network service providers, applications service providers and content applications service providers) as well as those utilising the services provided by the licensees. One of the objects of the CMA is to ensure information security and network reliability and integrity in Malaysia. The CMA: requires licensees to use their best endeavours to prevent network facilities or network services from being used for the commission of any offence under Malaysian laws; prohibits fraudulent or improper use of network facilities or network services; prohibits the use and possession of counterfeit access devices; prohibits use of equipment or device in order to obtain unauthorised access to any network services; and prohibits interception of any communications unless with lawful authority.

Computer Crimes Act 1997 (CCA)
The CCA criminalises: the act of gaining unauthorised access into computers or networks; spreading of malicious codes (e.g. viruses, worms and Trojan horses); unauthorised modification of any program or data on a computer; as well as wrongful communication of any means of access to a computer to an unauthorised person. Depending on the type of offence committed, the fine for a convicted offence ranges from RM25,000 to RM150,000 or imprisonment of three to 10 years or both. The case *Basheer Ahmad Maula Sahul Hameed v PP* [2016] 6 CLJ 422 (as discussed in 'Hacking' in question 1.1 above) is an example of an offence under the CCA.

Penal Code
In cases where computer-/internet-related crime activities are involved, but do not specifically fall within the ambit of any of the aforementioned statutes (for example, online fraud, cheating, criminal defamation, intimidation, gambling, pornography, etc.), such offences may be charged under the Penal Code, which is the main statute that deals with a wide range of criminal offences and procedures in Malaysia.

Personal Data Protection Act 2010 (PDPA)
The PDPA regulates the processing of personal data in commercial transactions and applies to anyone who processes and has control over or authorises the processing of any personal data in respect of commercial transactions.

The most relevant PDPA principle in the context of cybersecurity would be the Security Principle, i.e. appropriate technical and organisational security measures must be taken to prevent unauthorised or unlawful processing of personal data and accidental loss, misuse, modification or unauthorised disclosure of personal data.

The PDP Commissioner has also issued subsidiary legislation pursuant to the PDPA, among which are the Personal Data Protection Regulations 2013 (the "**Regulations**") and the Personal Data Protection Standard 2015 (the PDP Standards), which provide specific requirements regarding security standards expected of data users.

Copyright Act 1987 ("Copyright Act")
The Copyright Act generally protects copyrights, including trade secrets, intellectual property in devices or data, etc. Where any technological protection measure is applied to any copyright, it is an offence under the Copyright Act to circumvent such technological protection measures (section 36A of the Copyright Act). No person shall offer such technology or device which allows for circumvention of such technological protection measures, and non-compliance with the provision would be an offence and the person guilty of the offence may be held liable to a fine not exceeding RM 250,000 or to imprisonment for a term not exceeding five years, or to both; and for any subsequent offence, to a fine not exceeding RM 500,000 or to imprisonment for a term not exceeding 10 years, or to both.

Strategic Trade Act 2010 ("Strategic Trade Act")
The Strategic Trade Act 2010 is the legislation that controls the export, trans-shipment, transit and brokering of strategic items and

technology, as well as activities that will or may facilitate the design, development, production and delivery of weapons of mass destruction. The Strategic Trade Act, which is consistent with Malaysia's international obligations on national security, prohibits the import or export of strategic items, including items deemed as 'strategic technology' (i.e. controlled items as determined by the Minister of International Trade and Industry in Malaysia, such as encryption technology) (section 9 of the Strategic Trade Act).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The Malaysian Government, under the National Cyber Security Policy ("**NCSP**") has identified 10 critical sectors in Malaysia, known as the Critical National Information Infrastructure ("**CNII**"), which are required to be protected to a level commensurate with the risks faced. These CNII sectors are:

(1) National Defence and Security.
(2) Banking and Finance.
(3) Information and Communications.
(4) Energy.
(5) Transportation.
(6) Water.
(7) Health Services.
(8) Government.
(9) Emergency Services.
(10) Food and Agriculture.

While there are no minimum protective measures in general and across sectors to protect data and information technology systems from Incidents (save for security requirements in relation to personal data under the PDPA), the government of Malaysia has stipulated *ISO/IEC 27001 Information Security Management Systems* ("**ISMS**") as the baseline standard for information security and has proposed for all CNII sectors (as listed above) to be ISMS-certified. Such standards have been incorporated in certain sector-specific guidelines/handbooks. Penalties for failure to undertake such protective measures would be as prescribed by the respective standards/guidelines.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The PDPA regulates processing of personal data in the context of commercial transactions, including for the purpose of ensuring security of such data. Under the Regulations, organisations that process personal data (i.e. data users under the PDPA) are required to develop a security policy to ensure that personal data is protected from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Further to the above, the PDP Standards prescribe a list of minimum security standards to be complied with by the data users (e.g. prohibition of the use of removable media devices or cloud computing services for transfer or storage of personal data, unless with written authorisation from the top management of the organisation; ensuring the organisation's backup/recovery system and anti-virus software are regularly updated to protect personal data from data intrusion or security breach; and contractually binding third-party data processors in respect of data processing activities, etc.).

From the perspective of the CMA in turn, section 263 requires all network facilities or network service providers to use their best endeavours to prevent network facilities or network services, applications services or content applications services from being used in, or in relation to, the commission of any offence under any law of Malaysia.

Apart from the above, several sector-specific standards and guidelines also require organisations to apply security measures. Some examples of these are *BNM Policy Document on Risk Management in Technology* ("RMiT"), *BNM Guidelines on Data Management and Management Information System* ("MIS") *Framework for the Banking Sector*, the Securities Commission Malaysia's *Guidelines on Management of Cyber Risk*. These standards and guidelines will be further discussed below.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No such issues have arisen thus far in Malaysia.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There are currently no applicable laws in Malaysia that generally require organisations to report information related to Incidents or potential Incidents to a regulatory or other authority.

However, in August 2018, the PDP Commissioner published the Public Consultation Paper (No. 1/2018) entitled "The Implementation of Data Breach Notification" (the "**DBN Public Consultation Paper**") which would be applicable to organisations who are required to register under the PDPA and who process personal data or have control over or authorise the processing of any personal data (i.e. registered data users under the PDPA).

Pursuant to the DBN Public Consultation Paper, the PDP Commissioner intends to implement a data breach notification mechanism ("**DBN**") in Malaysia, where data users are required to notify and inform the relevant authorities and affected parties when a data breach has occurred within the organisation. Organisations will be required to report on:

(i) details about the Incident, (i.e. summary of the event and circumstances, type and amount of personal data involved in the Incident and the estimated number of affected individuals);
(ii) the organisation's containment or control measures (i.e. details of actions/measures taken or to be taken to contain the breach and the potential harm of the breach, especially to the affected individuals);
(iii) details and requirements with regards to notification (i.e. identification of the persons who have been notified about the

breach, details whether any regulatory bodies/law enforcement agencies have been notified about the breach, the method(s) used by the organisation to notify the affected individual about the Incident, any advice given to the affected individual, the requirement for the PDP Commissioner to be notified no later than 72 hours after having become aware of the breach); and

(iv) details on the organisations' training and guidance in relation to data protection (i.e. whether the organisation had provided training/awareness programmes to staff members prior to the Incident, whether the staff members involved in the Incident had received training in the last 24 months and whether the organisation had provided any detailed guidance to staff on the handling of personal data in relation to the reported Incident).

The DBN Public Consultation Paper in its current draft form merely provides that data users are to report to the authority and the affected/relevant parties where a breach has occurred in an organisation. However, the PDP Commissioner has not clarified the scope of such "breach" nor identified the events which would trigger reporting obligations, and whether any defences or exemptions exist by which the data subject might prevent publication of that information.

The DBN Public Consultation Paper has yet to come into force as at the time of writing.

Certain sector-specific guidelines have been issued imposing such requirements. Some examples are as follows:

- **Banking Sector**: *Policy Document on Risk Management in Technology* ("**RMiT**") prescribes the minimum standards on technology risk and cybersecurity management by financial institutions in Malaysia. It applies to financial institutions including licensed banks, investment banks, Islamic banks, insurers (including professional reinsurers), takaful operators (including professional retakaful operators), prescribed development financial institutions, approved issuers of electronic money, and operators of a designated payment system.

  Under the RMiT Policy Document, a financial institution must establish a comprehensive Cyber Incident Response Plan ("**CIRP**"), and the financial institution must immediately notify BNM of any cyber Incidents affecting the financial institution. Upon completion of investigation into the Incident, the financial institution is also required to submit a report on the Incident to BNM.
- **Capital Market**: *Securities Commission Malaysia's Guidelines on Management of Cyber Risk* sets out the roles and responsibilities of capital market entities, policies and procedures that should be developed and implemented, requirements for managing cyber risk and reporting requirements to the Securities Commission Malaysia. Under the said Guidelines, the capital market entities must report to the Securities Commission Malaysia on any detection of a cyber Incident impacting the entity's information assets or systems, on the same day of the Incident. The entities are also required to report any cyber breaches to the board of directors and periodically update the board on emerging cyber threats and their potential impact on the entity.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

While there are no general restrictions with regards to voluntary sharing of information pertaining to an Incident, this is subject to sector-specific regulations and regulatory oversight which may constrain an organisation from sharing such information. Additionally, where the information involves personal data, the organisation needs to make sure that the disclosure of the said personal data must fall within the exceptions under the PDPA.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There are currently no general requirements under Applicable Laws for organisations to report information relating to Incidents or potential Incidents to affected individuals. Notwithstanding the foregoing, the DBN Public Consultation Paper (which is currently in the public consultation stage, and pending formal issuance as discussed in question 2.5 above) requires organisations to provide information in relation to:

(i) details of actions/measures taken or to be taken to contain the breach;

(ii) advice given to the affected individual; and

(iii) the potential harm of the breach on the affected individuals and the method(s) used by the organisation to notify affected individuals about the Incident.

Apart from the general requirement for data users to report on data breach events, the DBN Public Consultation Paper has not specified the circumstances (i.e. what constitutes a "data breach") in which this reporting obligation is triggered.

Further to the above, certain sector-specific guidelines require the applicable organisations to implement policies or procedures to inform the relevant stakeholders of the Incident (e.g. the *SC Guidelines on Management of Cyber Risk* requires the relevant entity to implement communication procedures that will be activated by the entity in the event of a cyber breach, which include reporting procedures, information to be reported, communication channels, list of internal and external stakeholders and a communication timeline).

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, they do not.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regulators responsible for enforcing requirements are generally either sector-specific or subject matter-specific, including but not limited to:

Sector/Subject Matter	Relevant Statute/ Regulations	Regulator
Information Security / Network Reliability and Integrity	Communications and Multimedia Act 1998	Malaysian Communications and Multimedia Commission (**MCMC**)
Personal Data	Personal Data Protection Act 2010	Personal Data Protection Department /Commissioner's Office
Penal Offences	Penal Code, Computer Crimes Act 1997	Royal Malaysian Police
Sector-Specific Regulations	Banking and Financial Sector Guidelines	Central Bank of Malaysia or Bank Negara Malaysia (**BNM**)
	Securities Commission Guidelines	Securities Commission Malaysia (**SC**)

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Penalties for failure to comply with any of the abovementioned requirements are dependent upon the respective statutes, regulations or guidelines, for example:

- non-compliance with the PDPA may result in the organisation, upon conviction, to be liable to a maximum fine ranging from RM100,000 to RM500,000 or imprisonment ranging from one to three years, or both;
- non-compliance with the provisions under the CMA may result in the organisation, upon conviction, to be liable to a maximum fine ranging from RM50,000 to RM500,000 or imprisonment ranging from one to five years, or both;
- contravention with the provisions under the CCA or Penal Code would subject the organisation to enforcement by the Royal Malaysian Police, and may expose the organisation to liability involving a fine ranging from RM25,000 to RM150,000 or imprisonment of three to 10 years or both; or
- non-compliance with the relevant sector-specific guidelines may expose the organisation to enforcement actions by the relevant regulators (e.g. BNM or the SC), and may subject the organisation to regulatory sanctions such as a warning, public or private reprimands, an order to mitigate remedy the non-compliance, or even imposition of a monetary penalty). In cases involving severe non-compliance, the regulators may commence prosecution against the organisation.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There are no reported cases in Malaysian law journals in relation to any non-compliance of the abovementioned requirements.

From the regulatory perspective, regulators may impose regulatory sanctions on their licensees. These regulatory sanctions may be issued either privately (e.g. BNM) or publicly (e.g. MCMC) by regulators, depending on the regulator.

A listing of investigations and prosecutions is available on MCMC's official website.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no express restriction under Malaysian laws against an organisation using the above measure to detect and deflect Incidents in its own networks. While it may be open for discussion as to whether such measure contravenes the legal prohibition against interception of communication (pursuant to section 234 of the CMA, as discussed in our response to question 1.1 above), no such issue has arisen thus far in Malaysia.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Please see our response above.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Please see our response above.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

As stated in questions 2.3 and 2.5 above, apart from the PDP Standards which prescribe a list of minimum security standards to be complied with by data users, cybersecurity obligations and requirements vary across different sectors and are imposed in sector-specific legislation, regulations, standards and/or guidelines.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial services sector
BNM Policy Document on Risk Management in Technology ("**RMiT**")
BNM has issued the Policy Document on Risk Management in Technology (RMiT) which sets out the BNM's requirements with regard to financial institutions' management of technology risk. In complying with these requirements, a financial institution is expected to demonstrate risk management practices and controls that are commensurate with the increased technology risk exposure of the institution. The Policy Document also emphasises the need to ensure continuous availability of essential financial services to customers and adequate protection of customer data.

Under the RMiT Policy Document, a financial institution must establish a comprehensive Cyber Incident Response Plan (CIRP),

which include preparation, detection and analysis, containment, eradication and recovery; and post-Incident activity. When critical systems are outsourced or hosted by third party service providers, a financial institution has an obligation to regularly assess the adequacy of the provider's CIRP and its responsiveness to an attack.

Bank Negara Guidelines on Data Management and Management Information System ("**MIS**") Framework

These Guidelines set out several principles and elaborate on the specific safeguards to be applied for each principle. Among the safeguards required are that banks/financial institutions are to obtain the MS ISO/IEC 27001 Information Security Management Systems (ISMS) certification for critical systems, particularly the payment and settlement systems, to ensure that safeguards and security measures implemented over data and IT systems are effective.

Telecommunications sector

There are currently no specific cybersecurity obligations imposed on licensees under the CMA. However, under section 263 of the CMA, the Commission or other authority, may make requests in writing to its licensees requesting the licensees to assist the Commission or any other authority, as far as reasonably necessary, in preventing the committing or attempted committing of an offence under any written law of Malaysia, or otherwise in enforcing the laws of Malaysia, including the protection of the public revenue and preservation of national security.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Failure by a company to prevent, mitigate, manage or respond to an Incident would potentially give rise to a breach of directors' duties.

In the event of any breach or non-compliance of statutory requirements by the organisation, the directors may also be held jointly or severally liable for such breach or non-compliance.

Under section 133 of the PDPA, it is expressly provided that the commission of any offence by the body corporate may also render the officers of the body corporate (e.g. directors, the chief executive officer, managers, etc., who were responsible for the management of the affairs of the body corporate) to be charged severally or jointly with the body corporate, and in such instances may also be found to have committed the offence.

Directors may also be found liable for such failure under the relevant sector-specific standards or guidelines. For example, in the banking and financial sector, the *Guidelines on Data Management and MIS Framework* issued by BNM provide that senior management and the board of directors must play a key role in the development of a data management and management information system framework; and in capital markets sector, the *Guidelines on Management of Cyber Risk* issued by the SC set out the roles and responsibilities of the board of directors and management in the oversight and management of cyber risk. These provide that directors are subject to certain responsibilities and consequently may be held responsible for any non-compliance therewith.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no general requirement under Malaysian laws for companies to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments; and (d) perform penetration tests or vulnerability assessments. Requirements are generally sector-specific and in accordance with the relevant standards or guidelines (e.g. *SC Guidelines on Management of Cyber Risk* requires cyber risk policies and procedures to be implemented by the organisation, and sets out the required contents of such policies and procedures as well as an Incident response template).

Notwithstanding the above, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that a training/awareness programme and detailed guidance should be given to the organisation's staff for handling such Incidents.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies are not subject to general disclosure requirements in relation to cybersecurity risks or Incidents (whether to listing authorities, the market or otherwise in their annual reports).

Disclosure requirements in relation to cybersecurity risks or Incidents are sector-specific. For example, the *Guidelines on Management of Cyber Risk*, issued by the Securities Commission Malaysia, requires capital market entities to develop and implement cyber risk policies and procedures, which must include the strategy and measures to manage cyber risk encompassing prevention, detection and recovery from a cyber breach.

Notwithstanding the above, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that notification of Incidents must also be made to other regulatory bodies/law enforcement agencies.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Apart from the Applicable Laws (as set out at question 2.1 above), companies would also be subject to specific requirements in relation to cybersecurity under the relevant sector-specific standards or guidelines.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the event of an Incident, the company or organisation may be subject to civil actions on grounds of breach of contract or breach of statutory duties under the Applicable Laws (as set out at question 2.1 above).

In order to bring a claim on grounds of breach of contract, the claiming party must establish that there was a contractual duty in respect of cybersecurity (e.g. duty to protect confidential information or personal data), that there was a breach of such duty, and the loss or damage occasioned by such breach. A breach of statutory duty

in itself would give rise to a right to commence civil action, although the quantum of damages would be dependent on the extent of loss or damage suffered by the claiming party. The company or organisation may also be liable under tort, as set out in question 5.3 below.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

An example would be *Dynacraf Industries Sdn Bhd v Lee Kooi Khoon* [2008] 3 ILR 265, where an employer commenced action against a dismissed employee for alleged unauthorised interception and disclosure of electronic communication (in this case, another employee's private emails), in contravention with section 234 of the CMA (interception of communication). Apart from the foregoing, civil actions on grounds of copyright infringement or breach of confidence, have been brought in Malaysian courts.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

In the event of an Incident, the company or organisation may also potentially be exposed to tortious liability on grounds of negligence, as the aggrieved party may allege loss or damage as a result of the company's or organisation's breach of duty of care in relation to cybersecurity.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out cyber risk insurance against Incidents in Malaysia. Cyber risk insurance may either be first party coverage (i.e. to insure against loss and damage sustained by the insured, i.e. the organisation itself) or third-party coverage (i.e. to insure against liability for loss, damage or personal injury caused to a third person, namely the customers or clients of the organisation).

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no known regulatory limitations in respect of cyber risk insurance coverage. However, risk exposure due to the company's or organisation's own negligence or wilful default will likely be excluded by the insurer from the scope of insurance policy coverage.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no specific requirements under the Applicable Laws requiring monitoring of employees and for the employees to be under an obligation to report cyber risks, security flaws, Incidents, etc. to the employer. However, sector-specific guidelines may prescribe that employees be made aware of and understand the cyber risk policies procedures, the possible impact of cyber threats, as well as their roles in managing such threats (*Guidelines on Management of Cyber Risk*, issued by the Securities Commission Malaysia).

Additionally, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that a training/awareness programme and detailed guidance should be given to the organisation's staff for handling such Incidents.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no known Applicable Laws that may prohibit or limit the reporting of cyber risks, security flaws, Incidents by an employee, etc. In fact, the Whistleblower Protection Act 2010 ("**WPA**") was passed to encourage and facilitate the disclosures of improper conduct of companies or organisations by protecting the informants making such disclosures. It is further provided under section 6(5) of the WPA that any provision in any contract of employment which purports to preclude the employee from making a disclosure of improper conduct shall be to that extent void.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Royal Malaysian Police, the MCMC and other relevant regulatory authorities are granted wide investigatory powers under the relevant statutes (as set out in question 2.9 above).

In general, the law enforcement or regulatory authorities are authorised under the relevant statutes to exercise the following investigatory powers during an investigation:

- the power to investigate the relevant persons;
- search and seizure, by warrant or without warrant;
- request for access to computerised data;
- the power to intercept communications;
- the power to require the production of records, accounts, computerised data, documents, etc., and to make such inquiry as may be necessary to ascertain if the relevant statutory provisions have been complied with;
- the power to require attendance of persons acquainted with the case;
- examination of persons acquainted with the case; and
- the power to institute prosecution, with consent in writing of the Public Prosecutor.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

While there are no legal requirements under the Applicable Laws for organisations to implement backdoors in IT systems specifically for law enforcement authorities, several cybersecurity-related statutes provide the need for law enforcement authorities to be provided with the relevant encryption keys, passwords, decryption codes, software or hardware or any other means required in order to have access to computerised data during the course of investigations (section 249 of the CMA; section 10 of the CCA).

Deepak Pillai has practised exclusively in the areas of Telecommunications & Technology law and Personal Data Protection for two decades and is acknowledged as a leading Telecommunications & Technology lawyer in Malaysia.
Deepak advises clients on matters relating to IT contracts, electronic commerce, online financial services, outsourcing, telecommunications, IT security, personal data protection and digital media. He advises a wide array of international, private and public sector clientele in addressing the commercial, regulatory and policy issues relating to information and communications technology law, ranging from negotiating complex information technology contracts to advising public sector agencies on proposed technology related legislation and policies.
Described in *The Legal 500* over the years as "*the most recognised IT specialist in Malaysia", and "pioneering the practice of IT law as a discrete area of law in Malaysia*".
Deepak has been listed by the *Asia Pacific Legal 500* as a leading individual in the area of IT and Telecommunications from 2001 to date. Deepak is also currently listed in the 2019 edition of *Chambers Asia Pacific* as the sole practitioner in Band 1 for the area of Technology, Media and Telecoms.

Christopher & Lee Ong
Level 22, Axiata Tower, No. 9 Jalan Stesen Sentral 5
Kuala Lumpur Sentral, 50470
Kuala Lumpur
Malaysia

Tel: +603 2267 2675
Email: deepak.pillai@christopherleeong.com
URL: www.christopherleeong.com

Yong Shih Han practises exclusively in the areas of Technology, Media and Telecommunications (TMT), and Data Protection. Prior to joining the firm, she was a dispute resolution associate in a reputable firm handling primarily civil and corporate litigation matters. Since joining the firm and making the transition to corporate practice, she has been involved in the areas of corporate commercial, mergers & acquisitions, and general corporate advisory. She currently focuses on the areas of technology, media, telecommunications and data protection, with information security and data protection being her specialised area.
She now regularly advises clients on matters relating to information and communications technology, information security and data protection, telecommunications, and media and advertising laws. This ranges from the preparation and drafting of technology-related contracts and policies to advising clients on matters potentially leading to dispute resolution. She also regularly advises clients on technology- and media-related regulatory and compliance matters.
Shih Han has been listed by *The Legal 500 Asia Pacific* as a next-generation lawyer in the area of IT and Telecommunications in 2019.

Christopher & Lee Ong
Level 22, Axiata Tower, No. 9 Jalan Stesen Sentral 5
Kuala Lumpur Sentral, 50470
Kuala Lumpur
Malaysia

Tel: +603 2267 2715
Email: shih.han.yong@christopherleeong.com
URL: www.christopherleeong.com

Mexico

Creel, García-Cuéllar, Aiza y Enríquez, S.C.

Begoña Cancino

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

There is no definition in Mexican law of the terms "cybercrime" and "cybersecurity"; however, the Federal Criminal Code regulates illegal behaviours committed through electronic means that could be identified as cybercrimes by the use of electronic means for their commission.

Regarding examples of jurisdiction in Mexico, according to Article 16 of the Political Constitution of the United Mexican States ("Mexican Constitution"), no one shall be disturbed in his/her private affairs, family, home, papers or possessions (including private information), except by written order of a competent authority, duly grounded in law and fact, which sets forth the legal cause of the proceeding. In this regard, any non-consented access to private information may be sanctioned by law; thus, only a federal judicial authority may authorise any investigation regarding criminal offences.

Hacking (i.e. unauthorised access)
Article 211*bis* of the Federal Criminal Code provides that whoever, without authorisation, modifies, destroys or causes loss of information contained in systems or computer equipment protected by a security mechanism shall be imposed with a prison sentence of six months to two years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00. The aforementioned penalty could be duplicated in case the information is used for one's own benefit or to benefit a third party.

Denial-of-service attacks
The Federal Criminal Code does not provide any definition, or similar definition, for this criminal offence.

Phishing
The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered as fraud. According to Article 386 of the Federal Criminal Code, a person commits fraud when he/she, with the intent of obtaining a financial gain, handles information through deceit, takes advantage of errors, or misleads a person.

In such case, the relevant authority shall impose a prison sentence of three days to 12 years, as well as a fine of approximately MN$2,400.00 to MN$24,012.00, depending on the value in each case.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour is similar to hacking. The aforementioned penalties are applicable in this case.

In case the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one to four years, as well as a fine of approximately MN$16,000.00 to MN$48,024.00.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The Federal Criminal Code provides this criminal offence as "hacking", which is described above.

Identity theft or identity fraud (e.g. in connection with access devices)
The Credit Institutions Law provides that a person who produces, manufactures, reproduces, copies, prints, sells, trades or alters any credit card, debit card, cheques or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed a prison sentence of three to nine years, by the relevant authority, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00.

In addition, the Federal Criminal Code provides that a person who, with or without authorisation, modifies, destroys or causes loss of information contained in credit institutions' systems or computer equipment protected by a security mechanism shall be imposed with a prison sentence of six months to four years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00.

Moreover, a person who without authorisation knows or copies information in credit institutions' computer systems or equipment protected by a security mechanism shall be imposed a prison sentence of three months to two years, as well as a fine of approximately MN$4,002.00 to MN$24,012.00.

All the penalties aforementioned could be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
As mentioned, the Credit Institutions Law provides that any person who produces, manufactures, reproduces, copies, prints, sells, trades or alters, any credit card, debit card, cheque or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed with a prison sentence of three to nine years, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00. The aforementioned penalties may be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Yes: espionage; conspiracy; crimes against means of communication; tapping of communications; acts of corruption; extortion; and money laundering could be considered as threats to the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

Failure by an organisation to implement cybersecurity measures
Considering the absence of a specific law which regulates cybersecurity in Mexico, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Federal Law on Protection of Personal Data held by Private Parties ("Data Protection Law") provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes; however, Mexico has not yet adopted international standards related to cybersecurity.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, in the following cases:

1) The Federal Law Against Organized Crime provides: (a) that in the investigation of a crime in which it is assumed on good grounds that a member of organised crime is involved, it is possible to tap private communications; and (b) the obligation of concessionaires, authorised entities and any person holding a means or system that could be intercepted, to cooperate with the authorities, prior to a judicial order.
2) The General Law to Prevent and Sanction Kidnapping Crimes provides the possibility to intercept private communications.
3) The National Security Law, in case of an immediate threat to national security, provides that the Mexican government must request a judicial warrant to intercept private communications for national security purposes.
4) The Federal Telecommunications and Broadcasting Law ("FTBL"), according to Articles 189 and 190, provides that: (i) concessionaires; (ii) authorised entities; and (iii) service providers of applications or contents, are required to: a) allow the corresponding competent authorities to control and tap private communications; and b) provide the support that such authorities request, in terms of the applicable law.

In addition to the federal legislation provided above, there are state laws that allow the interception of individual communications prior to any request from the relevant state authorities (Public Prosecutor of the corresponding state) to a federal judge.

Intervention of private communications is not allowed in: electoral tax; commercial; civil; labour; or administrative matters, or in the case of communications between the arrested and his/her counsel.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

As mentioned, the Federal Criminal Code also regulates as a criminal offence the act of sabotage or unlawful interference with: roads, public services, or state services; steel, electric or basic industries; and centres of production or distribution of weapons, ammunition or military equipment, with the aim of disrupting the economic life of the country or to affect its ability to defend itself.

Also, the relevant Code protects means of communication such as telegrams, telephone lines, radio communications, telecommunication networks, and any component of an installation of production of magnetic or electromagnetic energy or its means of transmission.

In addition, the Federal Criminal Code provides that persons who manufacture, import, sell or lease any device or system, or commit any act with the purpose of decoding any encrypted/protected satellite signal without the legitimate authorisation of the licensed distributor, shall be imposed with a prison sentence of six months to four years.

On the other hand, the Law on Negotiable Instruments and Credit Operations sanctions diverse actions that affect any kind of financial payment instrument (e.g., credit or service cards) or the information contained on them.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- The Mexican Constitution.
- The FTBL.
- The Data Protection Law, its Regulations, Recommendations, Guidelines and similar regulations on data protection.
- The Federal Law on Transparency and Access to Public Information.
- The General Law on Transparency and Access to Public Information.
- General Standards as the Mexican Official Standard Regarding the Requirements that shall be Observed when Keeping Data Messages.
- The Law on Negotiable Instruments and Credit Operations.
- The Mexican Federal Tax Code.
- The Credit Institutions Law.
- The Sole Circular for Banks.
- The Industrial Property Law.
- The Mexican Copyright Law.
- The Federal Criminal Code.
- The National Security Law.
- The Federal Labour Law.
- The Federal Law for the Federal Police.
- The National Development Plan 2013–2018.
- The National Programme of Public Security 2014–2018.
- The National Programme of Security 2014–2018.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

This is not applicable in Mexico.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

As mentioned, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Data Privacy Law provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

In addition to the foregoing, there are certain specific mandatory security measures that certain industries must adopt to protect their customers' data. Banking laws and regulations provide that banks must implement certain security measures in electronic banking transactions and require the use of several passwords depending on the amount and nature of the transaction.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

This is not applicable in Mexico.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no obligation to report Incidents or potential Incidents to the authorities; however, the General Law on Transparency and Public Information Access provides, in Article 70 Section XLVII, that authorities must provide access and keep updated, for statistical purposes, the list of requests made to telecommunications concessionaires, service providers or internet applications related to the interception of private communications, access to the registry of communications, and the real-time geo-location of communication equipment, that contains the object, temporary scope and legal grounds of the request and, if applicable, a statement of judicial authorisation.

On the other hand, Data Privacy Laws do not provide a penalty for failure to comply with the rules on reporting threats or breaches; nevertheless, the National Institute for Access to Public Information and Data Protection ("INAI") is empowered to evaluate if the cause that originated a data breach was caused by a failure of compliance or negligence.

By the interpretation of the Mexican Constitution, organisations must cooperate with government agencies regarding Incidents; however, no law establishes specific requirements to report Incidents or potential Incidents.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Please refer to our answer in question 2.5.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There is no obligation to report any Incidents or potential Incidents; however, Data Protection Law provides that security breaches that materially affect the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses to questions 2.5 to 2.7 do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The INAI is in charge of: (i) guaranteeing people's right of access to public government information; (ii) protecting personal data in possession of the federal government and individuals; and (iii) resolving denials of access to information that the dependencies or entities of the federal government have formulated.

The Federal Telecommunications Institute ("IFT") is in charge of regulating telecommunications and broadcasting services.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The Applicable Laws are silent in this regard.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

This is not applicable in Mexico.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Answer not available at time of print.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. According to the Data Protection Law, the data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

On the other hand, the Federal Criminal Code and the Law on Negotiable Instruments and Credit Operations provide several sanctions in order to avoid criminal offences regarding cybersecurity.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes. Regarding financial services, the Law on Negotiable Instruments and Credit Operations and the Credit Institutions Law, including the Federal Criminal Code, are applicable in order to avoid cybercrimes.

The FTBL and the Federal Criminal Code are applicable in this matter.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are no specific laws in Mexico related to cybersecurity responsibilities or liabilities of personnel and directors. Nevertheless, and in accordance with the Data Protection Law, every private party, individual or organisation that processes personal information (data controller), has the obligation to appoint a data person or department (data protection officer) who will be a representative for the organisation in privacy and data protection matters and in charge, within the organisation, of the correct processing of personal data (including verification of security measures), as well as of processing requests from data owners for the exercise of their rights to access, rectification, suppression or rejection.

In relation to information security, data protection officers shall adopt measures to guarantee due processing of personal data, privileging the interests of the data owners and their reasonable expectation of privacy.

The measures that the data protection officer shall adopt, and that may be related to cybersecurity, include the following: (i) issuing policies and programmes, which shall be mandatory within the organisation; (ii) implementing training programmes; (iii) implementing a monitoring and surveillance system and internal or external audits to verify compliance with privacy policies; (iv) assigning resources for the implementation of programmes and policies related to privacy; (v) implementing a risk-detection programme to identify privacy risks when launching new products, services, technologies and business models as well as risk-mitigation strategies; (vi) periodically reviewing security policies and programmes to determine whether amendments are needed; (vii) performing compliance checks; and (viii) implementing personal data-tracking systems to trace which data are collected and where they are stored.

The Data Protection Law does not provide a specific sanction for data protection officers, responsible personnel and directors.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Regarding personal data, all data controllers must designate a data protection officer or department; however, the Applicable Laws are silent on cybersecurity matters.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The Applicable Laws are silent in this regard.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Applicable Laws are silent in this regard.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

According to Article 32 of the Federal Criminal Code, organisations and companies are civilly liable for the damages caused to third parties by crimes committed by their partners, managers and directors. The state is similarly liable for the crimes committed by its public officials.

The Federal Civil Code provides a standard of civil liability established in Article 1910, which provides that a party that illegally causes harm to another person shall be obliged to repair the damage, unless he/she proves that the damage was produced as a consequence of the victim's guilt or negligence.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

This is not applicable in Mexico.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

This is not applicable in Mexico.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in our jurisdiction.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

This is not applicable in Mexico.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no specific requirements; however, the Data Protection Law provides that a person who is involved with personal data is obligated to establish and maintain physical and technical administrative security measures and in case of any breach, such employee must notify the data protection officer.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

This is not applicable in Mexico.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) Public Prosecutors; (iii) the INAI; and (iv) the IFT.

Public Prosecutors in Mexico are in charge of investigating and resolving cyber activities; a cyber police service has been created to follow up on crimes or unlawful activities committed through the Internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account; in addition, the Federal Police have created a scientific division called the National Centre For Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyber threats and cyber attacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. The IFT is in charge of the telecommunications sector.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

The Applicable Laws are silent in this regard.

Begoña Cancino is a partner in the Mexico City office. Her practice focuses on Intellectual Property, Data Privacy, Regulatory and Administrative Litigation. From the standard IP front, Ms. Cancino counsels clients from all kinds of industries with the protection and enforcement of their IP rights in Mexico, assisting also with the transfer of IP portfolios within the context of complex corporate transactions involving all sort of IP rights (such as trademarks, copyrights and appellations of origin). Ms. Cancino also provides assistance with her legal advice on regulatory and advertising, assessing our clients to comply with all applicable provisions with COFEPRIS and PROFECO. She has represented clients in all sort of administrative litigation proceedings, in general, concerning advertising, health, environmental and, of course, IP matters, before administrative authorities and federal judicial courts. Pursuant to the data privacy aspects of her practice, Ms. Cancino has counselled clients from multiple industries in the drafting and implementation of internal policies, privacy notices and specific legal concerns, not only regarding client daily operations, but also within the context of cross-border transactions and internal investigations for compliance.

Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Pedregal 24, 24th Floor
Molino del Rey
11040, Mexico City
Mexico

Tel: +52 55 4748 0679
Email: begona.cancino@creel.mx
URL: www.creel.mx

Creel, García-Cuéllar, Aiza y Enríquez is an award-winning, full-service corporate law firm. It has over 80 years of experience in providing international and domestic clients with technical excellence, knowledge of the market and unparalleled client service. The firm is a strategic service provider to clients with the most complex and demanding transactions and projects, affording them certainty and peace of mind. The firm provides innovative solutions to many of the largest, most intricate, first-ever market-leading deals in Mexico. We are a full-service corporate law firm, specialising in the following practice areas and industries: antitrust and competition; arbitration and dispute resolution; banking and finance; bankruptcy and restructuring; capital markets; corporate and commercial; employment and labour; energy and natural resources; environmental; infrastructure; insurance and reinsurance; intellectual property; mergers and acquisitions; private equity; *pro bono*; project development and finance; real estate; social security; tax; telecommunications; and transportation.

www.creel.mx

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ

Norway


Christopher Sparre-Enger Clausen


Uros Tosinovic

Advokatfirmaet Thommessen AS

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Forced entry into data systems and access to data systems by unauthorised means, including hacking, is regarded as a criminal offence under Section 204 of the Norwegian Penal Code of 20 May 2005 (the "**Penal Code**"). Violations are punishable by fines or imprisonment for a term not exceeding two years.

Examples of prosecutions of the activities described in this question are also included in question 5.2 below.

Denial-of-service attacks
The serious hindering, without authorisation, by transferring, harming, deleting, deteriorating, altering or inputting information, without authorisation, and which may seriously disrupt or hinder the operation of a data system, is considered a criminal offence under Section 206 of the Penal Code. Denial-of-service attacks and distributed denial-of-service attacks will typically fall within the scope of Section 206 of the Penal Code. Violations are punishable by fines or imprisonment for a term not exceeding two years.

Phishing
The unauthorised use of another legal person's identity, identity papers, or the unauthorised use of information which may be easily confused with another legal person's identity, with the intent of (i) obtaining an unauthorised benefit for oneself or for another person, or (ii) inflicting a loss on another person, is regarded as an criminal offence under Section 202 of the Penal Code. Accordingly, this provision makes phishing a criminal offence. Violations of Section 202 of the Penal Code are punishable by fines or imprisonment for a term not exceeding two years.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The infection of IT systems with malware may constitute a criminal offence under several provisions of the Penal Code. Firstly, the possession of malware will as a rule be regarded as a criminal offence under Section 201 of the Penal Code. Section 201 of the Penal Code is further described below. Furthermore, the infection of IT systems with malware which may seriously disrupt or hinder the operation of an IT system, is – as further described above – regarded as a criminal offence under Section 206 of the Penal Code.

Lastly, any person who without authorisation changes, supplements, destroys, deletes or hides another person's data shall be guilty of vandalism under Section 351 of the Penal Code. Accordingly, the infection of IT systems with malware may be regarded as a criminal offence under Section 351 of the Penal Code. Violations of this provision are punishable with fines or imprisonment for a term not exceeding one year. Grand vandalism is punishable with imprisonment for a term not exceeding six years.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The unauthorised production, procurement, sale, use or distribution of (i) a computer password or other data which may give access to a data system or databased information, or (ii) a computer program or device which is suitable for the purpose of committing a criminal offence, with the intent that it be used for the purpose of committing a criminal offence, is punishable by fines or imprisonment for a term not exceeding one year under Section 201 of the Penal Code. Furthermore, the unauthorised procurement or production of a self-spreading data software is also punishable by fines or imprisonment for a term not exceeding one year under Section 201 of the Penal Code. Accordingly, the possession or use of hardware, software or other tools used to commit cybercrime (such as hacking tools) will in certain situations constitute a criminal offence in Norway.

Identity theft or identity fraud (e.g. in connection with access devices)
As mentioned above, the unauthorised use of another legal person's identity, identity papers, or the unauthorised use of information which may be easily confused with another legal person's identity, with the intent of (i) obtaining an unauthorised benefit for oneself or for another person, or (ii) inflicting a loss on another person, is regarded as an criminal offence under Section 202 of the Penal Code. Accordingly, identity theft or identity fraud is regarded as a criminal offence in Norway.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
There are no specific cybercrime provisions under Norwegian law which penalises electronic theft. The general prohibition against theft under Section 321 of the Penal Code only applies to theft of tangible property, and therefore does not apply to electronic theft. Electronic theft can, however, be penalised as forced entry into data systems and access to data systems by unauthorised means (but not the theft as such) under Section 204 of the Penal Code. Violations are punishable by fines or imprisonment for a term not exceeding two years.

Furthermore, both Section 207 and Section 208 of the Penal Code will to a certain extent criminalise electronic theft. Pursuant to Section 207 of the Penal Code, any person who has obtained knowledge or possession of a trade secret in the course of an assignment, honorary post, employment or business relationship, and which without authorisation (i) uses the trade secret, or (ii)

discloses the trade secret to another person, with the intent of enabling that person to make us of the trade secret, shall be punished with fines or imprisonment for a term not exceeding two years. The foregoing also applies to any person who in the course of an assignment, honorary post, employment or business relationship has been entrusted with technical specifications, descriptions, recipes, models or similar technical materials, and which unlawfully uses the aforementioned documentation during the course of his or her trade.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Violations of the right to private communication is regarded as a criminal offence under Section 205 of the Penal Code, and punishable with fines or imprisonment for a term not exceeding two years. Section 205 of the Penal Code, *inter alia*, applies to the unauthorised:

(i) through use of technical solutions, monitoring and wiretapping of telephone conversations or other communication between other persons, or negotiations held in private meetings which the offender did not participate in, or which the offender obtained without authorisation;
(ii) breaking of a protective measure and other access by unauthorised means to information which is transferred electronically or with technical equipment;
(iii) opening of a letter or other sealed written communication (e.g. encrypted emails or documents) which is addressed to another person than the offender, or other unauthorised access to such communication; or
(iv) hindering or delaying an addressee from receiving communication by hiding, changing, destroying or delaying the communication.

Failure by an organisation to implement cybersecurity measures

The failure by an organisation to implement cybersecurity measures does not constitute a criminal offence under the Penal Code.

We have, however, described and defined certain sector-specific Applicable Laws in question 2.1, which requires organisations to implement cybersecurity measures. The following Applicable Laws described in question 2.1 envisage criminal sanctions for the failure to implement cybersecurity measures:

A. **The Security Act** Section 11-4 penalises the failure to implement the cybersecurity measures required under the Security Act with fines or imprisonment for a term not exceeding six months.
B. **The Financial Supervision Act of 7 December 1956** Section 10 penalises the failure to implement the cybersecurity measures described in question 2.1C, below, with fines or imprisonment for a term not exceeding one year.
C. **The E-com Act** Section 12-4 penalises the failure to implement the cybersecurity measures described in question 2.1D, below, with fines or imprisonment for a term not exceeding six months.
D. **The Energy Act** Section 10-5 penalises the failure to implement cybersecurity measures required under the Emergency Regulation (as further described in question 2.1E, below), with fines or imprisonment for a term not exceeding one year.

However, the above-mentioned sanctions may only be imposed if the failure to implement the cybersecurity measure has been intentional or has been caused by gross negligence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Penal Code, albeit with several exceptions, mainly applies to activities carried out in Norway and in Norwegian jurisdictions. However, if the criminality of an act depends on or is influenced by any actual or intended effect, the act shall pursuant to Section 7 of the Penal Code be regarded as committed also where the effect has occurred or is intended to be produced. Accordingly, Section 202, and Sections 204–208 may have extraterritorial application, if the effect of the relevant offences occurred or was intended to occur in Norway, even if the criminal activity was initiated outside of Norway.

Section 201 of the Penal Code for the aforementioned reasons does not have extraterritorial application, as it only criminalises the unlawful possession and use of certain hacking tools without requiring the occurrence of an effect or the intended occurrence of an effect (e.g. access to an IT system).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The penalties described in question 1.1 above may be mitigated on the basis of Section 78 of the Penal Code. Mitigating factors of particular relevance in a cybersecurity context under Section 78 of the Penal Code are, *inter alia*, (i) that the offender has confessed that he or she has committed the crime, or (ii) that the offender has prevented, rectified or limited the damages caused by the offence, or tried to do so.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Section 99 and Section 101 of the Norwegian Copyright Act of 15 June 2018 (the "**Copyright Act**") prohibits the circumvention of technical protective measures for copyright protected works and computer programs. Violations of Section 99 and Section 101 of the Copyright Act are punishable with fines or imprisonment for a term not exceeding one year.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

There are currently no general Applicable Laws dedicated to cybersecurity in Norway. Accordingly, the regulatory cybersecurity landscape in Norway is fragmented and sector-specific. We have cited certain Applicable Laws of particular relevance below, and indicated which sector/area they apply to:

A. **The processing of personal data** is subject to:
   (i) the General Data Protection Regulation (Regulation (EU) 2016/679 – the "**GDPR**"); and
   (ii) the Personal Data Act of 15 June 2018.
B. **The public sector** is subject to:
   (i) the National Security Act of 1 June 2018 (the "**Security Act**").
C. **The financial services sector** is subject to the Regulation regarding the use of information and communication technology (the "**ICT Regulations**").
D. **Telecom providers** are subject to:
   (i) the Electronic Communications Act of 4 July 2003 (the "**E-com Act**"); and

(ii) the Electronic Communications Regulations of 16 February 2004 (the "**E-com Regulations**").

E. **The energy sector**, i.e. energy providers and entities that are comprised of the nationwide Power Supply Preparedness Organization (abbreviated as "**KBO**" in Norwegian), are subject to:
   (i) the Act relating to the energy and water resources sector in Norway of 29 June 1990 (the "**Energy Act**"); and
   (ii) the Regulation on Preventive Security and Preparedness in the Energy Supplies of 7 December 2012 ("**Emergency Regulations**").

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Network and Information Systems Directive (the "**NIS Directive**") has currently not been incorporated into the EEA Agreement, nor implemented into Norwegian law. The Norwegian Act which will implement the NIS Directive into Norwegian law is presently on hearing, but is not finalised and effective.

However, the Norwegian National Security Authority and Norwegian Ministries have the power to decide that the Security Act shall apply to undertakings which (i) processes classified information, (ii) is in possession or control of information, information systems, objects or infrastructure which are important to fundamental national functions, or (iii) is engaged in activities that are important to fundamental national functions.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

As mentioned in question 2.1, above, Norway has a number of Applicable Laws which require organisations to take measures to monitor, detect, prevent or mitigate Incidents. These Applicable Laws and some of the more relevant measures required to be taken under these Applicable Laws are described below:

A. **Data controllers and processors** under the GDPR are required to:
   (i) implement appropriate technical and organisation measures to ensure a level of security appropriate to the risk of the data processing;
   (ii) notify personal data breaches to the Norwegian Data Protection Authority (the "**NDPA**"); and
   (iii) notify data subjects of any personal data breach, provided that the breach is likely to result in a high risk to the rights and freedoms of natural persons.

B. **The public sector** under the Security Act is required to:
   (i) conduct regular risk assessments and tests concerning security risks;
   (ii) document its risk assessments and the security measures; and
   (iii) notify the Norwegian National Security Authority if (i) the public sector entity is affected, may be affected, or becomes aware of any planned or ongoing Incidents which may harm national security interests, or if (ii) there have been material infringements of the security requirements set out in the Security Act.

C. **Financial undertakings and similar organisations** under the ICT Regulation are required to:
   (i) establish Incident and change management procedures;
   (ii) ensure that the above-mentioned procedures are complied with; and
   (iii) notify the Financial Supervisory Authority of any Incidents that may result in a significant reduction of the functionality of the IT systems.

D. **Telecom providers** under the E-com Act and E-com Regulations are required to:
   (i) implement security measures for the protection of communications and data;
   (ii) notify subscribers/users and/or authorities of certain security breaches and risks of security breaches; and
   (iii) maintain confidentiality about the content of electronic communication and use of electronic communication.

E. **Energy suppliers** are required to:
   (i) establish routines for protecting and controlling access to sensitive information;
   (ii) secure and monitor the confidentiality, integrity and accessibility to digital information systems; and
   (iii) notify and report undesirable Incidents such as data breaches to the authorities.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The Applicable Laws described in question 2.1 are to a certain extent overlapping, and conflict of law issues may arise with respect to sector-specific legislation. However, there are no specific challenges regarding conflict of law issues within this area.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

As mentioned above, organisations under the Applicable Laws described in question 2.1 are required to report information related to Incidents to the relevant regulatory/supervisory authorities in Norway. The most generally applicable reporting requirement in Norway related to Incidents is set out in Article 33 of the GDPR, which we have detailed further below:

(a) The reporting obligation under GDPR Article 33 is triggered by a "personal data breach". Pursuant to GDPR Article 4(12), a "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(b) Personal data breaches are in Norway reported to the Norwegian Data Protection Authority (the "**NDPA**"). So-called "processors" (i.e. organisations which process personal data on behalf of controllers) are required to report the personal data breach to the "controller" (i.e. the organisation which determines the purpose and means of the processing of personal data).
(c) The report must at least:
  (i) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and personal data records concerned;
  (ii) communicate the name and contact details of the data protection officer or other contact point;
  (iii) describe the likely consequences of the personal data breach; and
  (iv) describe the measures taken or proposed to be taken by the controller to address the personal data breach.
(d) However, a controller is not obligated to report the personal data breach to the NDPA if it is unlikely that the personal data breach will result in a risk to the rights and freedoms of natural persons.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations may under Applicable Laws voluntarily share information related to Incidents or potential Incidents with relevant regulatory/supervisory authorities in Norway. However, the possibility of organisations sharing information related to Incidents or potential Incidents to regulatory authorities outside Norway, as well as other private sector organisations, may be limited by statutory confidentiality obligations and similar restrictions.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The following Applicable Laws described in question 2.1 require organisations to report information related to Incidents to affected individuals:

A. **GDPR Article 34** requires controllers to inform individuals of personal data breaches that are likely to result in a high risk to the rights and freedoms of the affected individuals (unless the reporting is excepted under GDPR Article 34(3)). The information provided to the affected individual should at least include the information listed in question 2.5 (c) items (ii)–(iv).
B. **Section 2-7 of the E-com Act** requires telecom providers to notify end users and subscribers of significant risks of security breaches, including security breaches which has (i) damaged or destroyed stored data, or (ii) violated the end user's or subscriber's right to privacy. However, a telecom provider is not obligated to report the aforementioned Incidents to affected individuals if the telecom provider is able to substantiate to the Norwegian Communication Authority that appropriate security measures has been implemented on the data affected by the Incident. Section 2-7 of the E-com Act does not set out the nature and scope of the information that is required to be reported.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses to questions 2.5–2.7 do not change if the notifications include the information provided in items (a)–(e). However, the GDPR may restrict organisations possibility to share the information provided in items (b)–(e), above, with regulatory authorities outside Norway, as well as private sector organisations in general. Any disclosures of price-sensitive information may be restricted by Norwegian competition legislation.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The following regulators are responsible for enforcing the requirements identified under questions 2.3 to 2.7:

A. **The Norwegian Data Protection Authority** is responsible for enforcing the requirements set out in the GDPR and the Norwegian privacy legislation.
B. **The Norwegian National Security Authority** is responsible for enforcing the requirements under the Security Act.
C. **The Norwegian Financial Supervisory Authority** is responsible for enforcing the requirements under the ICT Regulations.
D. **The Norwegian Communication Authority** is responsible for enforcing the E-com Act and E-com Regulations.
E. **The Norwegian Water Resources and Energy Directorate** is response for enforcing the requirements under the Energy Act and Emergency Regulations.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The regulators described in question 2.9 are furnished with the following rights with respect to penalties:

A. **The Norwegian Data Protection Authority** may impose administrative fines up to EUR 20,000,000, or in the case of an undertaking, 4% of the total worldwide annual turnover. However, infringements of the reporting requirements under the GDPR are limited to EUR 10,000,000, or in the case of an undertaking, 2% of the total worldwide annual turnover.
B. **The Norwegian National Security Authority** may, *inter alia*, impose coercive fines and administrative fines for any infringements of the Security Act.
C. **The Norwegian Financial Supervisory Authority** may impose coercive fines.
D. **The Norwegian Communication Authority** may, *inter alia*, impose coercive fines and administrative fines for any infringements of the E-com Act or E-com Regulations.
E. **The Norwegian Water Resources and Energy Directorate** may impose coercive fines and administrative fines for any infringements of the Emergency Regulations.

Please also see our answer to question 1.1 regarding penalties for failures by an organisation to implement cybersecurity measures, which also applies to this question.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Norwegian supervisory authorities have, to the best of our knowledge and to date, not taken any enforcement actions due to non-compliance with the above notification requirements. However, the NDPA has issued two noteworthy administrative fines for non-compliance with the security requirements under the GDPR:

A. The NDPA has notified the Municipality of Oslo (the Education Agency) of its intention to sanction the Municipality with a fine of NOK 2,000,000 for its infringement of the security requirements under the GDPR in connection with the Municipality's provision of the mobile application "Skolemelding".
B. The NDPA has sanctioned the Municipality of Bergen with a fine of NOK 1,600,000 for the Municipality's failure to implement adequate security measures on the computer systems relied upon by the elementary schools in the Municipality.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
An IP address will under Norwegian law be regarded as personal data if the organisation collecting the IP address has the means to identify the person using the IP address. Accordingly, the use of beacons, including for cybersecurity purposes, will be regulated by the GDPR and must have a legal basis under GDPR Article 6. The use of beacons will also be regulated by Section 2–7 b of the E-com Act, which stipulates that the affected user must be informed about the use of beacons, and consent to the use (such consent may be provided through the end user's web browser settings).

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Organisations are permitted to use honeypots under Norwegian law.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Organisations are permitted to use sinkholes under Norwegian law.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Please see our answer to question 2.1, which is also applicable to this question.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

As mentioned in relation to question 2.1 above, the financial sector is subject to the ICT Regulations. The telecommunication sector is subject to the E-com Act and the E-com Regulations.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Members of the board of corporations are liable for damages caused by negligence pursuant to the general compliance principles under Section 6-13 and 17-1 of the Norwegian Limited Liability Companies Act. Members of the board may therefore be held liable for not establishing appropriate security measures and/or otherwise prevent, mitigate, manage or respond to an Incident.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

In summary, the following companies are under the Applicable Laws described in question 2.1 required to implement the measures in items (a)–(d):

A. energy suppliers are under Section 2-2 of the Emergency Regulations required to designate a CISO;
B. telecom providers, financial undertakings, KBOs and public sector entities are required to establish a written Incident response plan or policy. Most companies processing personal data are also required to establish such plans under GDPR Article 32; and
C. (and D.) telecom providers, financial undertakings, KBOs, public sector entities and most companies processing personal data are required to conduct cyber risk assessment, including penetration tests and/or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Norwegian companies are not subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents. Listed Norwegian companies are generally obligated to disclose information which may be of significance to, e.g., the value of the shares, which in certain situations may require the listed company to disclose information in relation to cybersecurity risks and/or Incidents.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Please see our answer to question 2.3 where we have summarised other specific requirements under Applicable Laws in relation to cybersecurity.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In our assessment, the most significant exposure to civil actions in relation to any Incident arises out of the GDPR. Under GDPR Article 82, any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered. Furthermore, a person may under Section 30 of the Personal Data Act also claim damages for non-economic loss as a result of an infringement of the GDPR.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

We have below cited specific examples of cases that have been brought in Norway in relation to Incidents:
A. TBERG-2017-164611 (hacking/unauthorised access); and
B. TNERO-2013-89352 (several denial-of-service attacks).

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Any person who negligently or wilfully causes an Incident may under the Norwegian law of torts be held liable for any foreseeable loss which has occurred due to the negligent or wilful act.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations in Norway are permitted to take out insurance against Incidents.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are to the best of our knowledge no regulatory limitations on insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no specific requirements under Applicable Law regarding items (a) and (b), above.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The provisions on whistleblowing set out in the Working Environment Act of 17 June 2005 will in our assessment not limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee. However, the Regulations on employer's access to employees' email accounts, etc. of 2 July 2018 restricts a Norwegian employers' possibility to access employees' email accounts, personal folders on the company's IT systems, and devices used by the employees. The aforementioned Regulations may therefore potentially restrict Norwegian employers' possibility to identify Incidents or potential Incidents caused by an employee.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The law enforcement (i.e. the police and prosecution) authorities may, *inter alia*, rely upon the following investigatory powers under Criminal Procedure Act of 22 May 1981 (the "**Criminal Procedure Act**"):
(i) conduct a search of a person, location, vehicle and data systems;
(ii) confiscate evidence;
(iii) confiscate electronically stored data, including from providers of electronic communication services and networks; and
(iv) order any person who has dealings with a data system to provide information which is necessary to enable the law enforcement to access the data system (e.g. passwords and encryption keys).

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements under Applicable Laws for organisations to implement backdoors in their IT systems. However, pursuant to Section 199a of the Criminal Procedure Act, law enforcement authorities may in connection with searches of data systems order any person who has dealings with the data system to provide information which is necessary to enable the law enforcement authorities to access the data system, or to open it with biometric data.

Christopher Sparre-Enger Clausen heads Thommessen's Technology and Data Protection practice group and specialises within M&A, technology and data protection law. He has extensive experience from both domestic and international M&A and IT-projects, and regularly provide clients with legal and strategic advise within a broad range of areas relating to digitalisation and technology, such as data protection, cybersecurity, outsourcing, licensing, cloud computing, software development, as well as IP and regulatory matters pertaining to IT and telecommunications.

Advokatfirmaet Thommessen AS
Haakon VIIs gate 10
PO box 1484 Vika
NO-0116 Oslo
Norway

Tel: +47 23 11 11 41
Email: csc@thommessen.no
URL: www.thommessen.no

Uros Tosinovic is a senior associate in Thommessen's Technology and Data Protection practice group. He works with matters concerning technology, data protection and intellectual property. Uros is frequently engaged in large technology projects and complex data protection matters (including cross-border data transfer arrangements, risk assessments and data processing agreements). Uros also has considerable experience with matters pertaining to cybersecurity and copyright. Uros holds a Master's degree from the University of Oslo, with a master thesis on the legal protection of technological protection measures.

Advokatfirmaet Thommessen AS
Haakon VIIs gate 10
PO box 1484 Vika
NO-0116 Oslo
Norway

Tel: +47 23 11 14 44
Email: uto@thommessen.no
URL: www.thommessen.no

Established in 1856, Advokatfirmaet Thommessen AS is considered to be one of Norway's leading commercial law firms. The firm has offices in Oslo, Bergen, Stavanger and London. The firm provides advice to Norwegian and international companies as well as organisations in the public and private sectors, ranging from SMEs to large multi-national corporations. Thommessen covers all business-related fields of law.

As the world has undergone a technological revolution, our lawyers have very much been a part of the development of the industry along the way. We have assisted our clients and helped develop the framework necessary to adjust to new technological advances. Thommessen assists leading Norwegian and international companies, both on the customer and supplier side, in cases involving everything from IT procurement to development projects and licensing of technology and cybersecurity.

www.thommessen.no

THOMMESSEN

Poland


Mateusz Borkiewicz


Grzegorz Lesniewski


Joanna Szumilo

Lesniewski Borkiewicz & Partners (LB&P)

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is a criminal offence under Section 267 of the Polish Criminal Code. Anyone who, without being authorised to do so, acquires access to information not intended for him or her, by, *inter alia*, connecting to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information is liable to a fine (up to PLN 1,080,000.00), the restriction of liberty or imprisonment for up to two years. This also applies to anyone who acquires access to any part of a computer system without being authorised to do so.

Denial-of-service attacks
Denial-of-service attacks are a criminal offence under Section 269a of the Polish Criminal Code. Anyone who, without being authorised to do so, by transmitting, damaging, deleting, destroying or altering information data, significantly disrupts a computer system or telecommunications network is liable to imprisonment for up to five years. In some cases, DoS attacks can also constitute offences under Sections: 268 (hindering access to information); 268a (damaging databases due to interfering or preventing automatic collection and transmission of data or hindering access to data); and 269 (if the offence regards data that is of particular significance for national defence, transport, safety or the operation of the government or any other state authority or local government).

Phishing
Phishing is a criminal offence under Section 287 of the Polish Criminal Code. Anyone who, in order to achieve material benefits or to inflict damage upon another person, affects the automatic processing, collection or transmission of data or changes, deletes or introduces new entries, without being authorised to do so, is liable to imprisonment for up to five years. If phishing leads to identity theft or fraud, it may also be considered an offence under Section 190a of the Polish Criminal Code (see more below).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infecting IT systems with malware is a criminal offence under Section 287 of the Polish Criminal Code (for quotation see about phishing above). Moreover, according to Section 269 of the Polish Criminal Code, anyone who destroys, deletes or changes a record on a computer storage media that is of particular significance for national defence, transport, safety or the operation of the government or any other state authority or local government, or that interferes with or prevents the automatic collection and transmission of such information, is liable to imprisonment for up to eight years. Infection of IT systems with malware may be also a criminal offence if it results in at least one of the following: unauthorised access to information; destruction of information; damage to databases; denial of service; computer fraud (i.e. phishing); or disruption of work on a network.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit the offences specified above, including computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network, is liable to imprisonment for up to three years.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft or fraud is a criminal offence under Section 190a of the Polish Criminal Code. Anyone who pretends to be another person and uses his or her image, or other personal data, in order to cause property or personal damage may be subject to imprisonment for up to three years.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is a criminal offence under Section 266 of the Polish Criminal Code. Anyone who, in violation of the law or an obligation accepted, discloses or uses information learned in connection with the function or work performed, or public, social, economic or scientific activity pursued, is liable to a fine, the restriction of liberty or imprisonment for up to two years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Any transfer, disclosure or use of other entrepreneurs' information constituting business secrets, or acquiring such information from an unauthorised person, provided that it poses a threat to or violates an entrepreneur's interests, may be considered as an act of unfair competition under Section 11 of the Suppression of Unfair Competition Act.

Failure by an organisation to implement cybersecurity measures
Failure by an organisation to implement statutory obligations, including measures related to safety and cybersecurity, currently does not constitute a criminal offence. It can, however, be an administrative offence (e.g. under the GDPR). The company may also be subject to civil liability in case its negligent failure leads to damage. There is also a project of a new statute currently being processed – the Liability of Collective Entities Act – under which a company would be liable for criminal offences committed by managing bodies of the company or for criminal offences caused by deliberate or negligent acts or omissions by a member of the managing bodies of the company, e.g. due to failure to implement statutory obligations by the company (the offence must be directly related to the company's activity and scope of operation). The punishments will include financial penalties and dissolution of the company.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the listed offences are included in the Polish Criminal Code and although there are no specific regulations on extraterritorial application of these offences, the territorial application of the Polish Criminal Code depends on the place of the offence. The Polish Criminal Code (Sections 5 and 6, subsect. 2) is applicable when the offender acted or omitted an action to which they were obliged, or where the result occurred or should have occurred in accordance with the intention of the offender, or acted outside Poland but the result of one of the listed offences occurred in Poland, i.e. the offence affects IT systems located in Poland or systems used for providing services in Poland.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, there are general principles set out in the Polish Criminal Code and applicable to all the offences specified in it (including the offences listed above), which allow for mitigating penalties.

Section 59 – draw back – allows the court to draw back from imposing a penalty in case of milder offences.

Section 60 – extraordinary mitigation of punishment – allows the court to extraordinarily mitigate the punishment in cases indicated in a statute or in particularly justified cases when even the mildest punishment would be incommensurably harsh.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Under Section 165, subsect. 1 point 4 of the Polish Criminal Code, anyone who puts the lives or health of many people or possessions in danger by affecting computerised data commits a separate crime and may be sentenced for up to eight years of imprisonment. If any offence is committed due to or in relation to the offences listed above, the offender may be found guilty for committing several offences by one act, and if the offence is related to terrorism, the punishment may be even more severe.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

European Union – Key Applicable Laws:

1. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union;
2. Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification – under this regulation, soon there will be a uniform system of certification of cybersecurity of ICT in the EU – allowing for easier verification of the level of cybersecurity provided by organisations;
3. Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market;
4. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); and
5. Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

Key Polish Applicable Laws:

1. Criminal Code of 6 June 1997;
2. Labour Code of 26 June 1974;
3. Civil Code of 23 April 1964;
4. National Cybersecurity System Act of 5 July 2018 (NIS Directive implementation);
5. Trust Services and Electronic Identification Act of 5 September 2016;
6. Data Protection Act of 10 May 2018;
7. Suppression of Unfair Competition Act of 16 April 1993;
8. Telecommunications Law of 16 July 2004;
9. Counter-terrorism Act of 10 June 2016;
10. Crisis Management Act of 26 April 2007;
11. Payment Services Act of 19 August 2011;
12. Classified Information Protection Act of 5 August 2010; and
13. Recommendations and Instructions of Financial Supervision Commission concerning management of information technologies and security of the ICT environment.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Network and Information Systems Directive is implemented in Poland by the National Cybersecurity System Act of 5 July 2018 (NCS). However, there are some sectors of critical infrastructure that are wholly or partially regulated in other Applicable Laws: the trust services providers; health services providers established by the

Chief of Internal Security Agency or Chief of Foreign Intelligence Agency (i.e. Trust Services and Electronic Identification Act of 5 September 2016 and a set of regulations concerning some categories of health services providers); and telecommunication entrepreneurs referred to in the Telecommunications Law of 16 July 2004 (partially regulated in the NCS and partially the Telecommunications Law – in relation to cybersecurity requirements and Incident reporting).

Financial services providers are also subject to additional obligations regulated in statutes, which are specific for different kinds of financial service providers, e.g. for payment services providers: Payment Services Act of 19 August 2011 (implementing PSD2) – please also see the answer to question 3.2.

The NCS exceeds the requirements of the NIS Directive by including public administration, and partially the telecommunication sector, into the scope of the regulation. The NCS makes public administration provide at least the same standard of cybersecurity as operators of essential services and digital service providers, i.e. take measures to monitor, detect, prevent or mitigate Incidents at similar level as operators of essential services and digital service providers.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, organisations are required to undertake several activities to monitor, detect, prevent or mitigate Incidents. Under the National Cybersecurity System Act 2018 (NCS), operators of essential services shall implement a security management system for the information system used to provide the essential service that is relevant and proportionate to the estimated risk (having regard to the state of the art) and measures to prevent and minimise the impact of Incidents (examples are provided). Security audit of the information system must be carried out at least every two years. Under the NCS, digital service providers shall also face similar and relevant requirements.

In accordance with the Act on Provision of Electronic Services 2002, the service provider, in general, shall use appropriate cryptographic techniques.

In accordance with the Payment Services Act 2011, the provider, as part of the risk management system, takes risk mitigation measures and implements control mechanisms to manage risk through an effective Incident management procedure, including detection and classification of Incidents, including those related to ICT systems (e.g. strong user authentication).

In accordance with the GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (examples are given in Section 32, subsect. 1 of the GDPR).

In accordance with the Telecommunications Law 2004, the provider of publicly available telecommunications services is obligated to apply technical and organisational measures to ensure security and integrity of the network, services and transmission of messages in relation to the services provided and ensuring security of personal data processing (some duties are further specified).

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Conflict of laws may occur mainly between legislation of other countries, which shall be prevented by the implemented laws deciding on the applicability of specific rules.

Internal legislation has implemented a fairly efficient security model, with multiple overlaps and mutual complementarity. However, all entities should always exercise special caution when considering the extensive legal system, so their decision to satisfy the requirement of one act of law does not violate other laws.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, although depending on the type of organisation, the obligation may differ.

Operators of essential services, under the National Cybersecurity System Act, are required to report information related to Incidents to the appropriate CSIRT within 24 hours since the Incident was detected. The obligation is triggered when the operator of essential services classifies the Incident as serious. The notification about the Incident should contain basic information on the Incident, reporting person and entity and measures taken.

Organisations being digital services providers under the National Cybersecurity System Act have similar obligations.

Organisations from the financial sector who provide payment services are also required to report certain Incidents related to the payment services and possibly to cybersecurity. Depending on the type of provider, they are required to report to the Financial Supervision Commission (KNF), or another appropriate authority operational Incidents, Incidents related to security, Incidents involving account information service provider (AISP) and payment initiation service provider (PISP) and annual report on frauds related to payment services. The obligation is usually triggered by the sole occurrence of the Incident.

Telecommunications entrepreneurs are required to report to the President of the Electronic Communication Authority (*Prezes Urzędu Komunikacji Elektronicznej*) any breach of security or integrity of the network or services that had a significant effect on the functioning of the network or services, giving information on the breach and any preventive and corrective measures taken. The obligation is triggered by every significant breach.

Moreover, if the Incident has an effect on personal data processed by any organisation, such organisation is required to report such an Incident to the President of the Personal Data Protection Authority (*Prezes Urzędu Ochrony Danych Osobowych*).

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Sharing information related to Incidents or potential Incidents is not prohibited. Organisations are not required to but can voluntarily share such information but are required to comply with restrictions set out in other regulations – concerning personal data (GDPR) and confidentiality (including classified information – under the Classified Information Protection Act of 5 August 2010).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the GDPR, when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The communication shall describe in clear and plain language the nature of the personal data breach and contain basic information on the Incident specified in the Regulation.

There are situations when communication to the data subject may not be required.

Under the Act on Provision of Electronic Services 2002, the provider is obligated to ensure access by the customer to up-to-date information on special risks related to the use of the electronic service.

Under the Telecommunications Law 2004, when a personal data breach by a provider of publicly available telecommunications services may have adverse effects on the rights of the subscriber or end user who is a natural person, the provider shall immediately notify the breach to the subscriber or the end user with exceptions set out in the Telecommunications Law 2004, e.g. Section 174a subsect. 5.

The President of the Office of Electronic Communications (UKE) may impose on the telecommunications entrepreneur the obligation to publicly disclose the security or integrity breach of the network or services.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

In general, the answers are not subject to change.

In accordance with the Personal Data Protection Act 2018, the President of the Personal Data Protection Office, to perform his duties, has the right to access information that is a legally protected secret, including trade secrets.

It is similar under the National Cybersecurity System Act 2018 (NCS). The operator of essential services or the digital service provider includes in the Incident notice, to the extent necessary, information constituting a legally protected secret, including trade secrets, when it is necessary to perform the duties of the relevant CSIRT.

However, the circumstances given in the question may affect the possibility of publishing information to the public. Under the NCS, the relevant CSIRT may, after consultation with the notifying entity, publish specific information on serious Incidents when it is necessary to prevent an Incident or ensure Incident handling, or when for other reasons disclosing the Incident is in the public interest. Publication must not violate the rules on the protection of confidential information and other legally protected secrets or personal data protection rules.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

President of the Personal Data Protection Office (PUODO), www.uodo.gov.pl.

Ministers responsible for the relevant sectors – depending on the sector where the given operator of essential services or digital service provider operates, and one central body (Polish Financial Supervision Authority).

President of the Office of Electronic Communications (President of UKE), www.uke.gov.pl/.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Infringements of the provisions concerning personal data connected with cybersecurity issues shall be subject to administrative fines up to EUR 10,000,000.00, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Penalties stipulated by the National Cybersecurity System Act (NCS) may be up to PLN 200,000.00; however, if through an inspection of the body responsible for cybersecurity finds that the operator of essential services or digital service provider persists in breaching the NCS, it imposes a fine of up to PLN 1,000,000.00.

The body responsible for cybersecurity may also impose a fine on the managers of the operator of essential services (not exceeding 200% of their monthly salary) if they failed to exercise due care to meet specific obligations.

Penalties imposed by the Telecommunications Law may reach up to 3% of the income of the penalised entity generated in the previous calendar year (imposed both by the President of UKE and President of UODO, as applicable).

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In April 2019, the President of the Personal Data Protection Authority (PUODO) issued a PLN 55,750.50 fine to the Lower Silesian Football Association for unauthorised publishing on the Internet the personal data of people licensed as football referees in 2015. Published data included personal identification numbers and home addresses. It could have been avoided had the Association implemented requirements concerning technical and organisational measures in relation to the IT system used to process personal data [Decision ZSPR.440.43.2019 of 25 April 2019].

In March 2019, the President of the Personal Data Protection Authority (PUODO) issued a PLN 943,470.00 fine to a company which failed to provide information on personal data processing (Art. 14 of the GDPR) to the entrepreneurs whose personal data the company processed but lacked their e-mail addresses. This could have been avoided had the company implemented requirements concerning technical and organisational measures in relation to the IT system [Decision ZSPR.421.3.2018 of 15 March 2019].

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Yes. Currently there are no regulations prohibiting the use of beacons. However, the fact that beacons may acquire various information, e.g. IP, which may constitute personal data, all regulations concerning technologies, such as cookies and other similar solutions, apply to beacons.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Yes. There are no regulations prohibiting the use of honeypots. Moreover, NASK (*Narodowa Akademicka Sieć Komputerowa* – National Academic Computer Network – which is not only a research institute but also one of the three types of CSIRTs) is currently running a research project aimed at early identification and warning about cyberthreats based on honeypots.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Yes. Sinkholes may be used as a measure to detect and deflect Incidents and there are no regulations prohibiting such measures. They are, in fact, used by various organisations (e.g. in the telecommunications sector).

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice varies across different business sectors but there are no recognised deviations from the strict legal requirements. The differences between sectors depend rather on specific characteristics of the sector and the relevance of this sector. Some sectors, e.g. the financial services, telecommunications or new technologies sectors, are naturally more concerned and conscious about information security issues.

Also, under the National Cybersecurity System Act of 5 July 2018, public administration became part of the cybersecurity system and fell under further reporting guidelines and procedures, issued by the authorities of adequate level, in regulations other than the Applicable Laws.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes, there are specific legal requirements in both sectors.

(a) Financial services sector: detailed requirements concerning providing security of information in IT systems for providers of financial services are set out in the Recommendations and Instructions of Financial Supervision Commission (KNF) and specific statutes. In general, the providers are required to take measures to mitigate risk and develop control mechanisms aimed at risk management and security breach risk management.
(b) Telecommunications sector: companies are required (under Section 175, subsect. 1 of the Telecommunications Act) to take technical and organisational measures (providing a level of security appropriate to the risk, regarding the newest technological achievements and expected costs) aimed at providing security and integrity of the network, services and transfer of messages in relation to the provided services.

See also the answer to question 2.5.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Managers may be found liable towards the company if an Incident occurs due to their lack of due diligence (i.e. lack of internal procedures required in the given circumstances or failure to enforce them/lack of control if they are applied when they were responsible for compliance matters).

In some cases, a manager may be personally fined under the National Cybersecurity System Act – if, due to his/her negligence, the company that is an operator of an essential service failed to execute regular risk assessments and audits or fails to make proper notifications of the Incidents.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) No, however, under the National Cybersecurity System Act of 5 July 2018, companies which are operators of essential services are required to form an internal structure to ensure cybersecurity and designate a contact person to maintain contact with other state cybersecurity system elements.
(b) Operators of essential services are required to document cybersecurity measures related to the IT system used to provide essential services. Digital service providers are required to take measures allowing for risk management in relation to cybersecurity, but there is no obligation for a written form. Other companies are not required to establish any written Incident response plan or policy.
(c) Operators of essential services are required to conduct periodic cyber risk assessments and management of such risk and perform an audit at least once every two years. Digital service providers are required to take measures allowing for risk management – including monitoring, auditing and testing. Such measures may be necessary, under the GDPR, to any company processing personal data in IT systems – to ensure cybersecurity of such systems – including periodical risk assessment, testing and evaluation of taken technical and organisational measures.
(d) Please see the answers above.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies rendering electronic services must provide their clients with current information on any particular risks associated with the use of the electronic services provided.

Publicly traded companies must execute their duties on providing the market with current reports and periodic reports, and since cybersecurity risks or Incidents may have a significant effect on their financial or economic situation, they may be required to be disclosed.

The GDPR provides for a procedure on the reporting of Incidents concerning personal data protection (Section 33 of the GDPR).

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

In general, there is currently no other detailed requirements. However, companies are obliged to implement an IT security model.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The action related to civil liability may be brought against an offender (facing punishment and being liable for damages) or a company that failed to provide proper security measures against an Incident (liable for damages).

Action for damages – under Section 415 of the Polish Civil Code, action can be brought to compensate for actual damage (*damnum emergens*) and cost of opportunity (*lucrum cessans*). Section 444 of the Polish Civil Code allows for the claim damages to cover all costs related to the injury (e.g. medical care and drugs to treat the injury).

Action for compensation – under Section 445 of the Polish Civil Code, in addition to the claim for damages indicated above, the person who suffered injury may also be compensated for any harm suffered (including, e.g., psychological suffering). Under Section 448 of the Polish Civil Code for compensation to cover harm that resulted from the infringement of personal rights (e.g. damage to reputation).

There is also a possibility to bring a civil claim in criminal cases. Under Section 46 of the Polish Criminal Code, if the court convicts the offender, it may order the offender to partially or fully remedy any damage caused by the offence or compensate for any injury. The criminal court applies civil law provisions. This also applies when an offender commits an Incident-related offence (e.g. see the answer to question 1.1) and a person suffers damage or injury (e.g. in case the Incident involved a hospital) due to the offence.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

V CSK 141/17 (Supreme Court; 18 January 2018): the bank's client wanted to access her bank account through the internet. She entered her log-in data but was showed an information that the website is under maintenance. Later she discovered that the money she had was gone. It was determined in a separate (criminal) proceeding that a third person acquired her log-in data through phishing. The bank was found liable for not providing effective security measures and thus had to compensate for the damage the client suffered.

VI ACa 509/17 (Appeal Court in Warsaw, 30 August 2018): a third person accessed the bank account of a client of a bank and made several transactions for PLN 137,285.00 in total. The third person used the client's log-in data using the same IP address the client used on the same day. The bank used a two-factor authentication to send several messages (containing verification codes)– for the client to authorise the transactions. The client claimed that not all of the used codes were used by him. The client was not sure if his computer was properly secured (e.g. if the software was up to date). The court decided that in this case the client was negligent in taking security measures while using payment services provided by the bank. The court also pointed out that the bank provided effective security measures and could not be held liable for the loss of the client's money.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Civil liability is based on contract or tort – one does not exclude the other. Liability based on tort includes acts and omissions leading to damage (can be limited in contract) – regardless of whether there was a contractual obligation for specific acts or omissions.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. It is permitted and the cybersecurity insurance market is still developing. Taking out insurance against Incidents would also be treated as acting with due diligence while providing technical, organisational and legal measures concerning cybersecurity.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations concerning taking out insurance coverage against any type of Incident. However, insurance can only cover random Incidents – not planned or financed – which cannot be rationally excluded or mitigated.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

a) It is permissible only under some circumstances. Section 222, subsect. 1 of the Labour Code allows it if it is necessary, e.g., for providing employee's safety or property protection. Section 223 of the Labour Code allows for, e.g., monitoring of employee's

e-mails if it is necessary to ensure work organisation, allowing for proper management of full work-time and proper usage of working equipment made accessible to the employee. However, while monitoring employee's e-mails/computers, the employer has to comply with confidence of correspondence and other personal rights of the employee – which includes compliance with the GDPR.

b) It is not a statutory obligation for employees but under the statute implementing directive on whistle-blowers (still a project – see text here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0218), employers will have to implement internal rules/policies enabling whistle-blowers for reporting such flaws (and other breaches of law). The project of the statute is currently being processed.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are no regulations prohibiting or limiting reporting these. The employers will soon be required to implement adequate internal measures to allow whistle-blowing (unlawful acts and abuse of law) in accordance with regulations implementing the planned directive on whistle-blowers (see the answer to question 7.1). It is designed to cover all cyber risks, security flaws, Incidents or potential Incidents and secure the operating of a company (compliance).

Moreover, the National Cybersecurity System Act of 5 July 2018 allows for an entity (including companies, employees or any individual) to report Incidents, risks and security flaws to CSIRT NASK. Such voluntary notifications would be processed after all mandatory notifications had been processed.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Various governmental bodies have specific powers. Apart from the police or public prosecutors in criminal proceedings, note that the President of UODO, as part of their audit powers, is entitled to access buildings, premises or other spaces, to review documents and information that are directly related to the subject matter of the audit, and carry out inspection of places, objects, equipment, mediums and information systems and ICT systems used to process data.

In accordance with the National Cybersecurity System Act, a person carrying out inspections of entities that are businesses is entitled to free access to and moving around the premises of the audited entity without the obligation to obtain a security pass to inspect equipment, mediums and information systems.

Similar powers are also held by personnel of the Office of Electronic Communication that may also carry out inspections of the audited telecommunications networks and apparatuses.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes, under Section 179 of the Telecommunications Act, a telecommunications entrepreneur has to take technical and organisational measures of accessing and recording for the police and some other enforcement authorities to access and record telecommunications messages, sent or received by an end user, or terminal telecommunications equipment, and to access and record the metadata of such messages (messages include written, oral and other types of messages).

Under Section 9 of the Counter-terrorism Act of 10 June 2016, Chief of the Internal Security Agency may order for classified investigative operations concerning an individual who is not a Polish citizen, including getting access and recording data stored on a data storage device or terminal telecommunications equipment, IT systems and ICT systems.

Mateusz Borkiewicz has been advising since 2010. He was associated with one of the major law firms in Poland for almost five years, where he also held a managerial position with primary responsibility for the practices regarding GDPR and TMT industries in general.
He has advised on strategic topics concerning, among others, issues of unfair competition, protection of trademarks, cybersecurity, domain disputes, spam, violations of personal rights on the internet (particularly in the context of hate speech towards public figures), managerial bribery and computer crimes, including virtual currencies theft. At the same time, he was involved in *pro bono* projects in cooperation with the Helsinki Foundation for Human Rights.
He has served as Data Security Administrator and Data Protection Officer in several companies operating in the financial services, retail and automotive sectors.
He also entered into the list of attorneys kept by the District Bar Council in Wrocław, Poland.

Lesniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 663 683 888
Email: mb@lbplegal.com
URL: www.lbplegal.com/en

Grzegorz Lesniewski has been advising since 2009. His main areas of practice include personal data protection, the law of new technologies, cybersecurity and M&A.
For six years he was professionally connected with one of the major law firms in Poland, and for the last two years he has been managing the company's Warsaw office and was responsible for the TMT and M&A areas of specialisation. Later he developed the boutique law firm Leśniewski Legal, under which he advised on, among others, the implementation of GDPR by a Norwegian global provider of telecommunications and cable television services. He is also the Data Protection Officer at one of the major cloud computing companies in Poland since the entry of GDPR.
He managed the implementation of numerous M&A processes, as well as negotiations in the process of buying/selling companies mostly from the TMT sector.
He also entered into the list of attorneys kept by the District Bar Council in Warsaw, Poland.

Lesniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 531 871 707
Email: gl@lbplegal.com
URL: www.lbplegal.com/en

Joanna Szumilo has advised entrepreneurs and commercial partnerships, including providing ongoing support and design legal solutions for the IT industry since 2013. Besides graduating from the University of Wroclaw, she also studied law at British universities, i.e. Cambridge University (Diploma of Higher Education in Law and the Law of the European Union) and at University of Sussex, as well as psychology at the SWPS University of Social Sciences and Humanities (cognitive issues).
Joanna is a specialist in process strategies. She conducts proceedings regarding copyright and licensing of programming products – both in civil and criminal aspects. She designs new legal solutions and adapts existing ones to the needs of the information technology sector. She supports the protection of personal data and develops and implements internal procedures in the field of counteracting money laundering and financing of terrorism.
She also entered into the list of attorneys kept by the District Bar Council in Wrocław, Poland.

Lesniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 787 958 795
Email: js@lbplegal.com
URL: www.lbplegal.com/en

Lesniewski Borkiewicz & Partners (LB&P) is a modern law firm that works mainly with clients operating within IT, TMT and e-commerce. We know the specifics of the new technologies sector and that allows us to propose practical solutions, taking into account typical risks, market practice and upcoming changes. LB&P has been created as a result of the further development of Leśniewski Legal. It has been formed by people with experience gained in one of the largest Polish advisory companies, as well as in specialised projects realised for international clients.
Our second brand privacyfoxes.com is dedicated to GDPR issues and implementing solutions for cross-border personal data flows.

www.lbplegal.com/en

Leśniewski
Borkiewicz
& Partners

Portugal

Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.

Catarina Costa Ramos

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes; under the Cybercrime Law (Law no. 109/2009), access to a system or part of it without authorisation, to illegitimately produce, sell, distribute or generate a code or computer data that produces unauthorised actions, are offences punishable with one years' imprisonment or a fine.

Denial-of-service attacks
Yes; under the Cybercrime Law, unauthorised access with the objective of hindering, disrupting, obstructing or interrupting the normal activity of a computer by altering, deleting or damaging software or data and by any other method interfering with a computer, is punishable with a maximum sentence of five years' imprisonment or up to 600 daily fines.

When unauthorised access causes damage of considerably high value, or in case of a serious or lasting disturbance caused in a computer system which supports an activity aimed at ensuring critical social functions, i.e. the supply chains, health, safety and economic well-being of persons, or the regular functioning of public services, the penalty is imprisonment from one to 10 years.

Phishing
Yes; under the Cybercrime Law, actions with the intention of deception that interfere in a legal relationship, or actions such as the use of false data or obtainment of documents with the intention of having them used for legally relevant purposes, are punishable with a maximum sentence of five years' imprisonment or 120 to 600 daily fines.

The offence is punishable with one to five years' imprisonment when one of the actions mentioned above applies, regarding card data or any other system or means of payment, communications system or any system with limited access.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes; the infection of IT systems with malware would, in principle, be considered computer sabotage under the Cybercrime Law. Any action without authorisation with the objective of hindering or perturbing the normal functioning of IT systems through insertion, lodging, damage, change, deletion or denial of access to software or IT systems is punishable with a maximum sentence of five years' imprisonment or up to 600 daily fines.

For unauthorised access with the objective of intercepting transmissions of digital data within an informatics system, the sentence is up to three years' imprisonment or a fine. The attempt is also punishable.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Those who unlawfully produce, sell, distribute or in any other way disseminate or lodge one or more digital systems of software or computer data designed to commit the crimes foreseen in the Cybercrime Law, perpetrate a criminal offence, punishable with a sentence of up to one years' imprisonment or a fine.

If the possession is perpetrated through a violation of security rules, the sentence is up to three years' imprisonment or a fine; the sentence is up to one to five years when the agent, through the possession, has become aware of business secrets, industrial secrets or confidential data protected by law; or if the agent obtains considerably high profits.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes, under the Cybercrime Law, theft or identity fraud could, in principle, be considered "IT falsehood".

The actions to deceive and interfere with the processing of computer data with the objective of using false data or documents for relevant legal ends are punishable with a maximum sentence of five years or 120 to 600 daily fines. When these actions are about payment systems or communication systems, the sentence is one to five years' imprisonment. If the above-mentioned actions are perpetrated by an employee or a person in the performance of his duties, the sentence is up to two to five years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The copying, reproduction, selling, distribution or dissemination of software protected by copyright law is punishable with a maximum sentence of three years' imprisonment or a fine under the Cybercrime Law. The attempt is also punishable.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
The unlawful interception of data with the purpose of reproduction, selling, distribution or dissemination is punishable with a maximum sentence of three years' imprisonment or a fine under the Cybercrime Law. The attempt is also punishable.

Failure by an organisation to implement cybersecurity measures
Any legal person is criminally responsible for cybersecurity crimes under the Cybercrime Law, subject to the terms and limits established by the Portuguese Criminal Code.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The offences foreseen in the Cybercrime Law can be applicable to (i) offences perpetrated by Portuguese citizens if no other criminal law is applicable, (ii) offences that are committed to the benefit of legal persons based in Portugal, (iii) offences committed in Portuguese territory even though the target is a foreign IT system, or (iv) offences that are committed against IT systems in Portuguese territory regardless of where the offences are committed.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There is no exception or mitigation to any penalty foreseen in the Cybercrime Law. However, the court can decide to mitigate any penalty under the general rules of the Criminal Code.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

When related to terrorism, cybercrimes have more severe penalties under the Anti-Terrorism Law (Law no. 52/2003, August 22nd as amended by Law 16/2019, February 14th). Moreover, privacy intrusions through IT systems and swindling through computer data are criminal offences under the Criminal Code.

Additionally, other offences foreseen in the Criminal Code may apply; for example, embezzlement, fraud or theft.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The Portuguese legal framework for cybersecurity is dispersed across a variety of laws, as follows:

- the general legal framework for cybersecurity is Law no. 46/2018, August 13th (Cybersecurity Law), which transposes the Directive on security of network and information systems (NIS Directive) into Portuguese law;
- also applicable and complementing the NIS Directive, the Commission Implementing Regulation (EU) 2018/151, January 30th provides further requirements for digital service providers;
- in respect of cybercrime, complementing the Criminal Code, Law no. 109/2009, September 15th (Cybercrime Law) sets out cybercrime offences and communications surveillance and apprehension rules;
- the General Data Protection Regulation (GDPR) is applicable equally to Member States, although the European legislator has given space for the national legislator to legislate on some subjects, which complements the GDPR; the new Portuguese Data Protection Law, Law no. 58/2019, August 8th, is now applicable;
- the Electronic Communications Law (Law no. 5/2004, February 10th) is applicable to networks and service providers in electronic communications;
- also applicable, in respect of the identification and designation of critical infrastructure and the assessment of the need to improve its protection, is Decree-Law no. 62/2011, May 9th;
- the Electronic Commerce Law is applicable to electronic service providers (Decree-Law no. 7/2004, January 7th as amended by Law no. 46/2012, August 29th); and
- the competent Portuguese authority and computer security Incident response team (the national point of contact for cybersecurity under the NIS Directive) is the *Centro Nacional de Cibersegurança* (CNCS), governed by Decree-Law no. 3/2012, January 16th, establishing the National Security Cabinet, as amended by Decree-Law no. 136/2017, November 6th.

Also relevant is the security and integrity of electronic communications networks and services Regulation by ANACOM (National Communication Authority) and the ENSC 2019–2023 (National Strategy for Cybersecurity) Resolution of the council of ministers no. 92/2019.

Other legislation may apply with respect to civil and criminal matters.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Yes; in accordance with Law no. 46/2018 (the NIS Directive transposition law), operators of critical infrastructure shall have in place technical and organisational measures to ensure the security of networks and information systems. These measures should ensure a level of security proportional to the risks and take into account the latest technical advances.

Portuguese law does not impose further requirements than those in the NIS Directive.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The organisations that provide electronic communication services must adopt monitoring, detection, prevention and Incident mitigation, and business continuity plans, among others. The regulator might establish the following measures:

- a permanent point of contact;
- a chart of all the technical and organisational measures;
- evaluation exercises and drills; and
- an annual report.

Electronic service providers must retain one year's worth of electronic traffic and device location. Even though the European Court recognised differently (i.e. C 293/12 and C 594/12 (*Digital Rights Ireland*)), the Portuguese constitutional court, in 2017 (court judgment no. 420/2017), ruled that Portuguese law reflects all the necessary guarantees required by the ECJ in order to guarantee the proportionality of the retention.

Public organisations, critical infrastructure and digital providers must ensure an adequate security level, considering the risk at stake and technological advances, in order to reduce the risk of Incident, minimise impact, ensure business continuity, notify the competent authorities and evaluate the impact of any Incidents.

Digital providers must take into consideration:

- system and security facilities;
- Incident management;
- business continuity management;
- auditing, tests and monitoring; and
- compliance with international standards.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The Applicable Laws are largely harmonised at EU level and, as such, the risk of conflict of laws is minimised.

The identified requirements have exceptions in the applicable data protection and fundamental rights legislation, and the courts have evaluated the proportionality of such measures regarding such fundamental rights.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Public organisations and critical infrastructure operators, essential service operators and digital providers must notify any Incident having an impact on the provision of its services to the *Centro Nacional de Cibersegurança*; reporting, at least, the Incident's duration, the number of users affected, the geolocation of affected areas, the level of severity of the Incident and its impact on economic and social activities.

Such notification does not entail any further responsibilities for the notifying party.

Only substantial Incidents should be notified.

Should the Incident relate to personal data, the National Authority, *Comissão Nacional de Protecção de Dados*, should be notified if such Incident has an impact on the data subject's rights. Such notification should include a description of the nature of the personal data breach, including the categories and approximate number of data subjects concerned, the categories and approximate number of personal data records concerned, the name and contact details of the data protection officer, a description of the likely consequences of the personal data breach, and a description of the measures taken or proposed to be taken, including measures to mitigate its possible adverse effects.

Finally, regulated financial entities must report any relevant operational or security Incident to the respective supervisory authority, particularly when such Incident represents a risk to the entity and/or its clients.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Any organisation can voluntarily share information related to Incidents that have an impact on their services with the Portuguese Authority – *Centro Nacional de Cibersegurança*. The Portuguese Authority cannot impose any obligations on the organisation which it would not have imposed had it not been notified of the Incident.

Financial entities are also required to report to the pertaining supervisory authority any information that such authority might consider relevant to ascertain all the facts concerning an Incident affecting compliance with the applicable laws and regulations. All of this is subject to criteria of necessity and proportionality.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

In case of a personal data breach relating to personal data, the data subject should be notified without undue delay when that breach is likely to result in a high risk to the rights and freedoms of the data subject.

Such notification should include: a description, in a clear and plain language, of the nature of the personal data breach; the name and contact details of the data protection officer; a description of the likely consequences of the personal data breach; and a description of the measures taken or proposed to be taken, including measures to mitigate its possible adverse effects.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Please see questions 2.5 and 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regarding Public organisations and critical infrastructure operators, essential service operators, digital providers, the National Authority is the *Centro Nacional de Cibersegurança*, with headquarters at Rua da Junqueira 69, 1300-342 Lisboa; email: cncs@cncs.gov.pt / telephone number: +351 210 497 400.

Regarding the provision of Electronic Communications, the relevant Authority is ANACOM, with headquarters in Av. José Malhoa, 12; 1099-017 Lisboa; email: info@anacom.pt / telephone number: +351 217 211 000.

Regarding Incidents with an impact on personal data, the relevant authority is the Comissão Nacional de Protecção de Dados, with headquarters in Av. D. Carlos I, 134 – 1.º, 1200-651 Lisboa; email: geral@cnpd.pt / telephone number: +351 213 928 400.

Other supervisory entities might be involved – such as Bank of Portugal, the Insurance and Pension Funds supervisor authority, or the Portuguese Securities Market Authority – when applicable.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Regarding public organisations and critical infrastructure operators, essential service operators and digital providers not complying with the regulation, this might lead to a fine, which can range from €3,000 to €50,000 depending on the knowledge and intent of the parties.

Regarding the provision of electronic communications services, not complying with the regulation might lead to a fine which can range from €200 to €5,000,000, depending on the knowledge, size of the company, intent of the party and provision at stake.

Regarding personal data not complying with the regulation, this might lead to a fine under the terms of the GDPR (up to €20,000,000 or 4% of the company's or group's global turnover).

Other penalties might be applicable to financial entities depending on the specific sector, laws and regulations.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The above-mentioned requirements, with the exception of the electronics communication regulation, are part of a new legal framework; thus, enforcement decisions are scarce.

In 2019, to date, the National Authority, the *Comissão Nacional de Protecção de Dados,* has concluded three cases of administrative offences regarding non-compliance with GDPR – 21/2019 (for infringement of the right of access of the data subject), 207/2019 and 222/2019 (for infringement of the right to information of the data subject).

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

In accordance with Law no. 46/2018, organisations are permitted to define their own measures to detect and deflect Incidents in their own networks, taking into account the general principles established in the applicable law.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

Please see the answer above.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

Please see the answer above.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The Portuguese Cybersecurity Law does not impose specific security measures depending on business sectors, except those already mentioned.

However, some industries tend to invest more in information security, having dedicated teams. The financial services sector, the media sector and the sports sector, for example, have shown a growing concern for the implementation of further measures to prevent, detect, mitigate and respond to Incidents.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Electronic Communications Law imposes specific technical and organisational measures and reporting obligations on national authorities, and national security requirements on electronic communications network providers and/or electronic communications service providers.

The legal and regulatory framework for financial services imposes some specific requirements in relation to cybersecurity based on European laws, even imposing compliance with standard norms; for example, regarding measures concerning methods of payment on a case-by-case basis.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

The directors of a company have a general duty of care (duty to monitor). The duty of care (duty to monitor) might concern a director's duty to prevent, mitigate, manage or respond to an Incident. The Companies Code, in case of a breach, allows the director to be liable for damages caused by acts or omissions, unless they prove their innocence.

In regulated entities – insurance, banking and financial instruments – there are specific rules regarding corporate governance and, in particular, risk management and, therefore, the director may be liable for a breach of his obligations.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Even though the ISO/IEC 27001, ITIL and COBIT 5 frameworks are frequently used as standards for organisations to implement their own information security management systems, as well as providing some general guidance on the chief information security officer (CISO) framework for organisational structures, there is still a relatively low level of adoption of CISOs, which are mainly directed at large companies. Currently, there is no obligation to designate a CISO.

As mentioned in question 2.3, some organisations are required to: establish a written Incident response plan or policy; conduct periodic cyber risk assessments, including for third-party vendors; and perform penetration tests or vulnerability assessments.

As regards public administration in matters of network security and information systems, for personal data there are technical orientations given by the Resolution of the Council of Ministers no. 41/2018.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The applicable disclosure requirements are mentioned in question 2.5.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are specific requirements regarding the handling of classified information and its supporting systems, which might have an impact on cybersecurity requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Regarding an Incident, a civil liability action for damages may be brought under the general terms of the Portuguese Civil Code.

In order to obtain compensation from the responsible party or subcontractor for damages suffered by the plaintiff, the fact that caused them harm must be attributable to the defendant.

Furthermore, a person who suffers damage in relation to an Incident caused by lack of action of the Authority, may bring an action claiming both for compensation and for the Authority to act.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

One example is the ruling of 14/12/2016 of the Portuguese Supreme Court of Justice on the process 1063/12.1TVLSB.L1.S1 regarding a civil action of a company against a bank after a "phishing" attack, where the bank paid due compensation amounting to the value stolen through the Incident and to moral damages, having found that the bank had not undertaken all the necessary measures.

Another example following the above reasoning, the Guimarães Court of Appeal ruled on the proceeding 2406/17.7T8BCL.G1 emphasising that the "phishing" attack was not the client's fault.

The Court concluded that it was the bank who did not undertake all the necessary measures to prevent the attack, sentenced to pay compensation amounting to the stolen value, plus a compensation for the non-material damage suffered.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

There is potential liability in relation to an Incident, since there is, as mentioned above, a specific duty to maintain the safety of the information; accordingly, there is a claim for compensation if there is a breach in the duty of the defendant towards the plaintiff resulting in an injury.

However, the claims may vary according to the existence of a contractual relation and the type of torts (intentional torts, negligent torts and strict liability torts).

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber insurance is available on the Portuguese insurance market.

Nevertheless, under the Insurance Contract Law, insurers are prohibited from covering i) criminal liability or administrative fines, ii) the risk of crimes against personal liberty (such as kidnapping), iii) possession or transport of unlawful drugs, and iv) death of children under the age of 14 years old or of people with a psychological anomaly or another cause of inability to govern oneself.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Please see question 6.1 above.

Additionally, Portuguese general rules on compensation do not comprise consequential losses.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The employer is generally free to establish rules of conduct for its employees through internal regulation.

However, as regards the monitoring of employees and the reporting of Incidents, several requirements should be met, namely: the employees should have prior knowledge of the monitoring; the monitoring should not occur in order to find employees' wrongdoing; and the control should not constitute continuous monitoring of the employees' activities and should not have the purpose of evaluating

employees' performance. The monitoring should be random and not directed at a specific employee, and the employer should grant all means for the employees to follow the established rules.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are currently no applicable labour laws limiting the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee.

However, in order for such reporting to be legally required, it should be established in the internal rules of conduct and the employees should be granted the means in order to fulfil such requirement. If the reporting is legally demanded, the employer could eventually sanction an employee who does not follow such instruction.

It is recommended for the employer, in order to legally demand the report, to provide confidentiality and safety measures for the reporting of Incidents or potential Incidents.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The most relevant laws attributing investigative powers to both the regulators and to law enforcement to investigate an Incident are, besides those already mentioned in question 2.1, the following:

- Law of Cybercrime (Law no. 109/2009, September 15th).
- Portuguese Criminal Code.
- Anti-Terrorism Law (Law no. 52/2003, August 22nd, in compliance with Council Framework Decision 2002/475/JHA, June 13th, as last amended by Law no. 16/2019, February 14th).
- Internal Security Law (Law no. 53/2008, August 29th, as amended by Law no. 21/2019, February 25th).

An example of attributed investigative powers is the interception of communications for criminal cases, and investigation of a crime committed by means of a computer system or for which it is necessary to collect evidence in an electronic format.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

The Judgment of the Constitutional Court no. 413/2015, which set aside the rule that allowed the Secret Information Services to access "metadata" as well as tax and banking information, started a doctrinal debate on the limits of the investigative power.

Law no. 4/2017, August 25th, was approved in order to allow the Secret Information Services not only to access the information mentioned above, but also to intercept communications even through covert actions, provided that they are duly supervised.

Even though such powers allow for law enforcement to access some equipment, or the data generated, there are no specific requirements for the implementation of backdoors.

Catarina Costa Ramos is a Managing Associate at Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L. (GPA), working in the areas of data protection, aspects of cybersecurity and commercial contracts.
She has 19 years of experience advising and representing companies in the areas of corporate law, labour law, GDPR, consumer protection, intellectual property, commercial contracts and other applicable legal and regulatory frameworks, including cybersecurity.
Catarina is a GDPR/data protection trainer and she is a speaker at data protection conferences.

Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Edifício Amoreiras Square
Rua Carlos Alberto da Mota Pinto, Nº 17 – 3º B
1070-313 Lisbon
Portugal

Tel: +351 213 121 550
Email: catarina.ramos@gpasa.pt
URL: www.gpasa.pt

Singapore


Rajesh Sreenivasan


Justin Lee


Yu Peiyi

Rajah & Tann Singapore LLP

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

According to the applicable legislation specified below, the following activities would constitute criminal offences in Singapore.

Hacking (i.e. unauthorised access)
Yes. Under section 3 of the Computer Misuse Act ("**CMA**"), any person who knowingly causes a computer to perform any function for the purposes of securing access without authority to any program or data held in any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years, or to both.

In *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1999] 3 SLR(R) 653, the accused relied on an exploit, instead of sophisticated software, to perform unauthorised access to an internet service provider server, among others.

In *Lim Siong Khee v Public Prosecutor* [2001] 1 SLR(R) 631, the accused hacked the victim's email account by answering correctly the hint question to successfully retrieve passwords and to gain unauthorised access. He was sentenced to 12 months' imprisonment.

Denial-of-service attacks
Yes. Under section 7(1) of the CMA, any person who knowingly and without authority or lawful excuse (a) interferes with, interrupts or obstructs the lawful use of a computer, or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in computer, shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

There have been no prosecutions for denial-of-service attacks as yet. Nevertheless, such attacks are recognised as threats under Singapore's Cybersecurity Strategy.

Phishing
There is no specific provision that deals with phishing. However, under section 3 of the CMA, any person who knowingly causes a computer to perform any function for the purposes of securing access without authority to any program or data held in any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years, or to both.

In July 2018, there was a prosecution relating to multiple phishing activities, and it was reported that the offender was sentenced to three years and five months' imprisonment, and fined S$5,000.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes. Under section 5 of the CMA, a person who commits any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Yes. Under section 8B of the CMA, it is an offence for a person to obtain or retain any item (which includes hacking tools, among others) with the intent to use it to commit or facilitate commission of an offence under the CMA.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes. Under section 4 of the CMA, it is an offence to secure unauthorised access to any computer program or data, with the intent to commit an offence involving property, fraud or dishonesty. This offence is punishable on conviction by a fine not exceeding S$50,000 or imprisonment for a term not exceeding 10 years, or to both.

In *Public Prosecutor v S Kalai Magal Naidu* [2006] SGDC 226, the accused was convicted under section 4 for conducting searches on her bank employer's computer systems to effect cash withdrawals from the victim's bank account. She was sentenced to four months' imprisonment for each charge under section 4.

Also, under section 5 of the CMA, an accused may be charged for unauthorised modification of computer material. This may be seen in *Public Prosecutor v Tan Hock Keong Benjamin* [2014] SGDC 16, where

the accused used the victim's debit card that he found to make a purchase on eBay. It was held that he knew that by doing so, he would cause unauthorised modification to the contents of a computer, namely the data stored in the bank's servers, such that the online purchase would be approved.

In addition, the Penal Code contains provisions on cheating by personation. Although not cyber-specific, section 416 of the Penal Code (cheating by personation) may apply to identity theft. It is an offence for anyone to cheat by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. The punishment is imprisonment for a term of up to five years, a fine, or both.

In addition, under section 170 of the Penal Code, it is an offence to personate a public servant. The punishment is imprisonment for a term which may extend to two years or a fine, or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Under section 8A of the CMA, it is an offence for a person to obtain or retain personal information, or to supply, offer to supply, transmit or make available the personal information, if the person knows or has reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of the CMA. This offence is punishable on conviction by a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

The theft of personal data could also constitute an offence under the Personal Data Protection Act 2012 ("**PDPA**"). Under section 51 of the PDPA, it is an offence for an organisation or individual to dispose of, alter, falsify, conceal or destroy personal data. The punishment for this offence is a fine of up to S$5,000 in the case of an individual, and up to S$50,000 in any other case.

Under section 136 of the Copyright Act, the following instances of copyright infringement are criminal offences, where the infringing party knows or ought reasonably to know that the copies are infringing ones: make for sale or hire infringing copies; sell or let for hire infringing copies; possess or import infringing copies for commercial purposes; and distribute infringing copies for commercial purposes.

There is also criminal liability if the copyright infringement is wilful and either or both of the following two situations apply: (i) the extent of the infringement is significant; and/or (ii) the person does the act to obtain a commercial advantage.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Under the CMA, it is an offence to perform unauthorised use or interception of a computer service (section 6), and for unauthorised disclosure of an access code (section 8). Attempts are also caught under section 10 of the CMA, whereby anyone who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under the CMA shall be guilty of an offence. Therefore, any forms of attempts to gain unauthorised access, or to commit any other offences under the CMA, will constitute offences as well.

Failure by an organisation to implement cybersecurity measures

The PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. If the organisation does not comply with this requirement, the Personal Data Protection Commission ("**PDPC**") can give the organisation directions to ensure compliance; for example, directing the organisation to pay a financial penalty of up to S$1 million.

The Cybersecurity Act 2018 (No. 9 of 2018) ("**CSA**") requires owners of designated critical information infrastructure ("**CII**") to audit the compliance of their CII with the CSA and the applicable codes of practice and standards of performance at least once every two years, and conduct a cybersecurity risk assessment of the CII at least once a year. Any CII owner which does not comply shall be guilty of an offence and shall be liable on conviction to a fine not exceeding S$100,000 or to imprisonment for a term not exceeding two years, or to both.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The CSA, CMA, and PDPA have extraterritorial application.

The CSA applies to any CII located wholly or partly in Singapore.

Section 11 of the CMA specifies that the CMA provisions have effect against any person, irrespective of nationality or citizenship, even if the person is outside or within Singapore, if:

(a) the accused was in Singapore at the material time of the offence;
(b) the computer, program or data was in Singapore at the material time of the offence; or
(c) the offence causes or creates significant risk of serious harm in Singapore.

The above captures anyone who commits an offence under the CMA for which the person targets a computer, program or data located in Singapore, or if the person was in Singapore when the offence happened. Also, if the offence causes significant risk of serious harm in Singapore, then the extraterritorial provision may apply. Examples of serious harm include the disruption or serious diminution of public confidence in essential services such as communications and transport infrastructure or public utilities.

The PDPA applies to activities relating to the collection, use and disclosure of personal data in Singapore, and may apply to an individual, company, association or body of persons, corporate or unincorporated whether or not formed or recognised under the law of Singapore, or resident, or having an office or a place of business, in Singapore.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The legislations do not specify mitigating factors to the above offences. Nevertheless, cooperation with the relevant regulators or enforcement authorities, or active steps taken to mitigate the loss or damage caused by any of the offences, could be viewed by the courts or in the case of a breach of PDPA, the PDPC, as mitigating factors.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

In addition to legislation specifically targeted at cybercrime, the existing criminal offences as set out in the Penal Code and Sedition Act (Cap. 290), among others, may be able to encompass offences relating to cybersecurity. It is generally an offence (even though not specific to cybersecurity) to commit or facilitate terrorism activities, e.g., where there is financing of terrorism.

The Protection from Harassment Act (Cap. 256A) (the "**POHA**") establishes that it is an offence to intentionally cause harassment, alarm or distress, and to commit unlawful stalking. For example, unlawful stalking includes keeping the victim or a related person under surveillance.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The current laws which relate to cybersecurity in Singapore include:

Cybersecurity Act 2018 (No. 9 of 2018) (CSA)
The provisions of the CSA relating to CII came into operation on 31 August 2018. The CSA establishes a framework for the oversight and maintenance of national cybersecurity in Singapore and imposes duties and obligations on owners of CII.

Computer Misuse Act (Cap. 50A) (CMA)
The CMA sets out penalties for various cybersecurity offences, as described in section 1 above. Depending on the offence, the maximum quantum of the fine ranges from between S$5,000 to S$50,000, and the maximum imprisonment term ranges from between two and 10 years. The penalties may be enhanced in specific circumstances. For example, the maximum fine quantum and imprisonment term are increased in the case of second or subsequent convictions.

Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA)
The PDPA imposes data protection obligations on private organisations when they perform activities involving the collection, use and disclosure of personal data. The PDPC has powers to bring enforcement actions against organisations which fail to comply with these PDPA obligations.

Penal Code (Cap. 224)
As described in section 1 above, the Penal Code sets out offences relating to personation, among others.

Copyright Act (Cap. 63)
As described in section 1 above, the Copyright Act establishes that certain acts of copyright infringement constitute offences.

Strategic Goods (Control) Act (Cap. 300)
The Strategic Goods (Control) Act controls the transfer and brokering of strategic goods and strategic goods technology (including specified information security and cryptographic systems), among others.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

In the CSA, there are cybersecurity requirements that impose duties on owners of CII. Per the CSA, CII refers to a computer or computer system that is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore. The Commissioner will have the power to designate a computer or computer system as a CII.

'Essential services' are specified in the First Schedule of the Act. The First Schedule details 46 types of services which may be considered as 'essential services', under the broad categories of energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, Government, and media.

Section 9 of the CMA enhances the punishment for certain offences that are committed on protected computers (including computers used for defence, communications, public utilities, and banking, among others). The applicable punishment is increased to a maximum fine of up to S$100,000, and/or imprisonment for a term not exceeding 20 years.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Protection Obligation imposed by the PDPA, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Under the CSA, CII owners will be required to: comply with such codes of practice, standards of performance, or directions in relation to the CII as may be issued by the Commissioner; carry out regular audits and risk assessments; and participate in cybersecurity exercises as required by the Commissioner.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No such issues have been reported to have arisen thus far in Singapore.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Personal Data Protection Act 2012 (PDPA)
The PDPA does not currently contain any mandatory reporting obligations for Incidents or potential Incidents. However, on 22 May 2019, the PDPC issued the "Guide to Managing Data Breaches 2.0" ("**Guide 2.0**"). While the Guide 2.0 is non-binding in nature, it sets out the PDPC's position on data breach notification – the PDPC expects to be notified of data breaches that meet the relevant

notification thresholds (discussed below), in anticipation of a mandatory breach notification requirement being eventually introduced into the PDPA. Data breach notifications made by organisations or the lack thereof, as well as whether organisations have adequate recovery procedures in place, will affect the PDPC's assessment of any Incident or data breach, including its decision as to whether an organisation has reasonably protected the personal data in its possession or under its control.

(a) An organisation is expected to notify the PDPC of an Incident or other data breach that is (i) likely to result in significant harm or impact to the individuals to whom the information relate, or (ii) of a significant scale (i.e. involving personal data of 500 or more individuals). The organisation is expected to notify PDPC as soon as practicable, and no later than 72 hours after establishing that the data breach is one that meets either of the notification thresholds.
(b) The regulatory authority to which the Incident or data breach is to be reported is the PDPC.
(c) The nature and scope of information required to be reported would include: extent of the data breach; type(s) and volume of personal data involved; cause or suspected cause of the breach; whether the breach has been rectified; measures and processes that the organisation had put in place at the time of the breach; information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so; and contact details of person(s) whom the PDPC can contact for further information or clarification.
(d) No express defences or exemptions exist by which the organisation might prevent publication of the information disclosed to the PDPC. In practice, the organisation can nevertheless notify the PDPC which portions of the information are commercially sensitive or confidential to the organisation and the PDPC may take that into account when publicly disclosing information about the data breach.

Cybersecurity Act 2018 ("CSA")

The CSA imposes a duty on CII owners to report cybersecurity Incidents to the Commissioner of Cybersecurity if these Incidents involve CII or systems interconnected with CII. The information required for reporting (and corresponding time limits) are prescribed by the Commissioner and include the nature, cause, and impact of the Incident, and the remedial measures taken.

The CSA also grants the Commissioner powers to investigate all cybersecurity threats and Incidents (not only those involving CIIs); for example, to obtain information (such as technical logs), and, in the event of serious cybersecurity threats and Incidents, to enter premises where relevant computers and computer systems are located, access such computers, and scan computers for cybersecurity vulnerabilities.

In addition, the Commissioner will be empowered to direct any person or organisation to take emergency measures and requirements to prevent, detect or counter any threat to essential services or the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

While there are no general restrictions with regards to voluntary sharing of information pertaining to an Incident, this is subject to sector-specific regulations and regulatory oversight which may constrain an organisation from sharing such information.

If the information pertains to personal data, the organisation must comply with the PDPA in sharing such information.

Additionally, organisations should not share information protected on the grounds of it being a national secret or which is prejudicial to national security, under the Official Secrets Act and Internal Security Act, respectively.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

As discussed in response to question 2.5 above, the Guide 2.0 sets out the PDPC's expectations of organisations in respect of Incidents and other data breaches.

(a) Per the Guide 2.0, an organisation should notify the affected individuals of an Incident or other data breach where the breach is likely to result in significant harm or impact to the individuals to whom the information relate. Notification should take place as soon as practicable. This is to allow the affected individuals the opportunity to take steps to protect themselves from the risks of harm or impact from the data breach. If an organisation is uncertain whether affected individuals should be notified, the Guide 2.0 provides that they should seek clarification from the PDPC.
(b) The nature and scope of information required to be reported would include: how and when the data breach occurred; types of personal data involved in the data breach; what the organisation has done or will be doing in response to the risks brought about by the data breach; specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused; contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or websites); and/or where applicable, what type of harm/impact the individual may suffer from the compromised data.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses do not change, provided that any PDPA requirements are complied with if the information includes personal data.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regulators responsible for enforcing requirements are generally either sector-specific or subject matter-specific, including but not limited to:

Sector/ Subject Matter	Relevant Statute/Regulations	Regulators
Cybersecurity	**CSA**, CMA	Ministry of Communications and Information ("**MCI**"), Cyber Security Agency of Singapore
Personal Data	PDPA	PDPC
Penal Offences	Penal Code	Singapore Police Force ("**SPF**")
Sector-Specific Regulations	Banking and Financial Sector Laws/Notices/Guidelines	Monetary Authority of Singapore ("**MAS**")
	Telecommunications Act	Infocomm Media Development Authority ("**IMDA**")

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Penalties for failure to comply with any of the abovementioned requirements are dependent upon the respective statutes, regulations or guidelines, for example:

- The PDPC has powers to issue directions and bring enforcement actions to ensure compliance with the PDPA and can impose a financial penalty of up to S$1 million.
- Under section 14 of the CSA, a CII owner who fails to notify the Commissioner of a prescribed cybersecurity Incident in respect of the CII within the prescribed period after becoming aware of such occurrence, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding two years, or to both.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The PDPC has taken an active role in ensuring action be taken against organisations which breach the PDPA. By way of example, on 21 April 2016, the PDPC imposed financial penalties of S$50,000 and S$10,000 on K Box Entertainment Group ("**K Box**") and its data intermediary, Finantech Holdings, for failing to implement proper and adequate protective measures to secure its IT system, resulting in unauthorised disclosure of the personal data of 317,000 K Box members. K Box was also issued directions and penalised for the absence of a Data Protection Officer.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

In the "Guide to Securing Personal Data in Electronic Medium", the PDPC recommends organisations to implement defences which may be used to improve security of networks, such as: (a) Intrusion Prevention Systems ("**IPS**") (a device or software application that monitors network or system activities and prevents malicious activities or policy violations); (b) Intrusion Detection Systems ("**IDS**") (a network security appliance that monitors network and system activities for malicious activities and may raise alerts upon detecting unusual activities); and/or (c) web proxies, anti-virus and anti-spyware software. In this regard, a "Beacon", "Honeypot" or "Sinkhole" that falls within the scope of an IDS, IPS or other anti-spyware software is likely to be permissible.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Apart from the PDPA requirement for all organisations to make reasonable security arrangements to protect personal data, other cybersecurity obligations and requirements are imposed in sector-specific legislation, codes of practice, and guidelines, such that information security measures vary depending on business sector.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial services sector

Under the Technology Risk Management Notices, regulated financial institutions are required to notify the MAS as soon as possible, but no later than one hour, upon the discovery of a relevant Incident. Regulated financial institutions are required to submit a root cause and impact analysis report to the MAS, within 14 days or such longer period as the MAS may allow, from the discovery of the relevant Incident.

A 'relevant Incident' refers to a system malfunction or IT security Incident, which has a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers.

The MAS has also issued guidelines for financial institutions to mitigate cybersecurity risks, such as the Technology Risk Management Guidelines, Outsourcing Guidelines, Business Continuity Management Guidelines, and Bring-Your-Own-Device ("**BYOD**") Circular.

In September 2018, the MAS issued a public consultation regarding the Notice on Cyber Hygiene, regarding MAS' intention to issue a Notice on Cyber Hygiene, which prescribes a set of essential cybersecurity practices that financial institutions must put in place to manage cyber threats.

Telecommunications sector

The IMDA has formulated the Telecommunication Cybersecurity Code of Practice to enhance the cybersecurity preparedness for designated licensees. Besides security Incident management requirements, the Code also includes requirements to prevent, protect, detect and respond to cybersecurity threats.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Failure by a company to prevent, mitigate, manage or respond to an Incident could amount to a breach of directors' duties; for example, if the failure results from a director's breach of their duty to act honestly and use reasonable diligence in the discharge of the duties of their office.

While not mandatory, the Code of Corporate Governance ("**Code**") sets out best practices in relation to corporate governance principles. The Code of Corporate Governance is issued by the MAS, on recommendation by the Corporate Governance Council, and was last revised on 6 August 2018. Under Principle 9 "Risk Management and Internal Controls", the board of directors is responsible for the governance of risk and should ensure that management maintains a sound system of risk management and internal controls, to safeguard the interests of the company and its shareholders.

In relation to financial institutions, the MAS has issued the Technology Risk Management Guidelines, which set out technology risk management best practices and recommend that, in view of the importance of the IT function in supporting a financial institution's business, the board of directors and senior management should have oversight of technology risks and ensure that the organisation's IT function is capable of supporting its business strategies and objectives. The board of directors and senior management should ensure that a sound and robust technology risk management framework is established and maintained. They should also be fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is currently no general requirement under Applicable Laws for all companies to designate a CISO. However, under the PDPA, organisations are required to designate at least one individual, the data protection officer ("**DPO**"), to oversee data protection responsibilities within the organisation and ensure compliance with PDPA.

(b) There is currently no general requirement under Applicable Laws for all companies to establish a written Incident response plan or policy. However, the Guide 2.0 provides that whether an organisation has an adequate Incident response plan in place is one of the factors that will affect the PDPC's decision as to whether an organisation has reasonably protected the personal data in its possession or under its control.

(c) There is currently no general requirement under Applicable Laws for all companies to conduct periodic cyber risk assessments. However, in non-binding guidelines, PDPC recommends organisations to conduct a review of their cybersecurity risks and security measures regularly to ensure that they are up-to-date.

(d) There is currently no general requirement under Applicable Laws for all companies to perform penetration tests or vulnerability assessments.

In addition, there may be sector-specific cybersecurity requirements. For example, in relation to financial institutions, the MAS Technology Risk Management Guidelines recommend that financial institutions devise an Incident response framework, perform risk assessments, as well as penetration tests and vulnerability assessments. The MAS Outsourcing Guidelines recommend that financial institutions conduct periodic risk assessments on outsourced service providers, and review and monitor the security practices and control processes of the outsourced service providers on a regular basis.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies are currently not subject to specific disclosure requirements in relation to cybersecurity risks or Incidents (whether to listing authorities, the market or otherwise in their annual reports).

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Companies may be subject to specific cybersecurity requirements under sector-specific codes or guidelines, such as those set out in section 3 above.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

An Incident could give rise to claims in contract (for breach of contract) or tort (as set out under question 5.3 below).

The PDPA provides for a right of private action, whereby any person who suffers loss or damage directly as a result of a contravention of certain Data Protection Provisions by an organisation shall have a right of action for relief in civil proceedings in a court. In such a private action, the court may grant the plaintiff all or any of the following: (a) relief by way of injunction or declaration; (b) damages; and/or (c) such other relief as the court thinks fit.

Under the CMA, the court may order a person convicted of a CMA offence to pay compensation to any victim of the offence. This order will not prejudice the victim's right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There have not been reported cases directly relating to civil actions brought in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A party may face potential liability in tort in relation to an Incident; for example: if the Incident results from the party's negligence, there is a breach of confidence, or there is a breach of statutory duties.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Organisations are permitted to take out insurance against Incidents. Often known as 'cyber insurance', such insurance may cover business interruption loss due to network security failure or attack, human errors, or programming errors, among others.

As this type of insurance is relatively novel in Singapore, it has been reported that the MAS and CSA have been working with industry partners and a Singapore university to research on cyber risk, security and insurance, so as to develop insurance schemes to protect citizens and businesses against cyber attacks.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Currently, there are no regulatory limitations to insurance coverage against the specified losses, such as business interruption, system failures, cyber extortion or digital asset restoration.

Notwithstanding the above, the general rule of *ex turpi causa non oritur actio* applies to insurance contracts as it applies to contractual illegality. A person cannot rely on his own illegal act to make a claim against his insurance policy, nor benefit from his own criminal conduct. This is also contrary to public policy, since allowing the indemnification of such risks would be to encourage the commission of crimes, which would be wholly against public policy.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) Generally, the Applicable Law does not impose specific requirements on employers to monitor employees for the purposes of preventing, detecting, mitigating and responding to Incidents.

In relation to financial institutions, the MAS Technology Risk Management Guidelines recommend that, for accountability and identification of unauthorised access, financial institutions should ensure that records of user access are uniquely identified and logged for audit and review purposes. The MAS recommends that financial institutions should closely supervise staff with elevated system access entitlements and have all their system's activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures.

In the non-binding Advisory Guidelines issued by the PDPC, which provide examples of security arrangements to protect personal data, the PDPC recommends restricting employee access to confidential documents on a need-to-know basis.

(b) There are no requirements under Applicable Law regarding the reporting of Incidents or potential Incidents by employees to their employers. However, it is to be noted that under the employment contracts or internal company policies, there may be such notification requirements imposed upon employees.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are currently no Applicable Laws which may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

CMA: computer misuse offences are investigated by the SPF. More specifically, within SPF's Criminal Investigation Department, the Technology Crime Division conducts investigation and forensic examination into technology-related offences committed under the CMA. The SPF's powers of investigation are set out under the Criminal Procedure Code (Cap. 63) ("**CPC**").

PDPA: the PDPC can initiate investigations upon complaint or its own motion. It has the power to require relevant documents or information, and the power to enter premises without warrant as well as under warrant.

Internal Security Act ("**ISA**"): in the interest of Singapore's national security, the ISA provides for the Government's power to order preventive detention, and the power of police to search and seize subversive documents, among other powers.

CSA: the Act grants investigative powers to the Cybersecurity Commissioner (or any other cybersecurity officer upon his authorisation) and permits the exercise of powers necessary to determine the impact or potential impact of the cybersecurity threat or Incident.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under section 40(2) of the CPC, for the purposes of investigating an arrestable offence, the Public Prosecutor may by order authorise a police officer or an authorised person to require any person, whom he reasonably suspects to be in possession of any decryption information, to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence. Failure to comply is an offence punishable by a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years, or to both.

Under the CSA, the Minister for Communications and Information has the power to issue directions to any person or organisation to take such measures, such as the exercise of powers referred to under section 40(2) of the CPC to require decryption information, as may be necessary to prevent, detect or counter any serious and imminent cyber threat to essential services, national security, defence, foreign relations, economy, public health, public safety or the public order of Singapore.

Rajesh Sreenivasan heads the Technology Media and Telecommunications Practice at Rajah & Tann Singapore LLP. He has been advising clients on matters relating to cybersecurity, data protection, telecommunications, electronic commerce, IT contracts, digital forensics and digital media for over 20 years.

His clients include financial institutions, state governments, multinational corporations in the telecoms, computer hardware and software sectors, government-linked companies and statutory boards. On the regional front, Rajesh has been engaged by the ASEAN Secretariat to facilitate a pan-ASEAN forum on legislative and regulatory reforms to collectively address convergence of IT, telecoms and broadcasting across all 10 member countries, and by the Commonwealth Secretariat to co-lead an e-government capacity building exercise involving all member Caribbean nations. Rajesh has also been the contributing author for the Singapore chapter of Sweet & Maxwell's *Data Protection Laws of the World* since 2010. Rajesh has been cited as a leading TMT lawyer by all major legal ranking directories.

Rajah & Tann Singapore LLP
9 Straits View #06-07
Marina One West Tower
Singapore 018937

Tel: +65 6232 0751
Email: rajesh@rajahtann.com
URL: sg.rajahtannasia.com

Justin Lee has been a part of Rajah & Tann Singapore LLP's Technology, Media and Telecommunications, practice group since 2015. An integral member of the team, Justin has advised and assisted numerous clients on a wide range of legal and compliance matters, including issues relating to data protection, cybersecurity, intellectual property, IT contracting and telecommunications. Notably, Justin has also been appointed by the Singapore Personal Data Protection Commission ("**PDPC**") to assist in its industry outreach and education efforts, and has conducted several data protection briefing sessions on behalf of the PDPC.

Rajah & Tann Singapore LLP
9 Straits View #06-07
Marina One West Tower
Singapore 018937

Tel: +65 6232 0453
Fax: +65 6428 2230
Email: justin.lee@rajahtann.com
URL: sg.rajahtannasia.com

Yu Peiyi joined Rajah & Tann Singapore LLP's Technology, Media and Telecommunications practice group in 2019. He has advised and assisted clients on legal and compliance matters relating to personal data protection, cybersecurity, media, intellectual property and telecommunications.

Rajah & Tann Singapore LLP
9 Straits View #06-07
Marina One West Tower
Singapore 018937

Tel: +65 6232 0971
Fax: +65 6428 9302
Email: peiyi.yu@rajahtann.com
URL: sg.rajahtannasia.com

Rajah & Tann Singapore LLP has grown to be one of the largest full-service law firms in Singapore, providing full service and high-quality advice to an impressive list of clients. We have more than 300 lawyers, many ranked among the very best in their specialist practice areas.

Our Technology, Media and Telecommunications ("**TMT**") Practice is at the forefront of the TMT sector as thought leaders and trusted legal advisors for major TMT organisations and regulatory bodies in the Asia Pacific region and beyond. Led by a team of Partners who have been universally commended as the best of breed in TMT and ably supported by a team of specialist Associates, we are ready to help our clients navigate through this dynamic and constantly evolving area of practice.

Cybersecurity is a key area of concern for all clients, and safeguarding clients' trust and ensuring confidentiality of sensitive data is a vital task for many of our clients. In this respect, our broad suite of cybersecurity services, which includes multi-disciplinary data breach services and 24-hour emergency response teams, stand ready to assist our clients as may be required.

sg.rajahtannasia.com

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

South Africa


Fatima Ameer-Mia


Christoff Pienaar


Nikita Kekana

Cliffe Dekker Hofmeyr

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

At present, the current legal framework relating to cybercrime and cybersecurity in South Africa is a hybrid of different pieces of legislation and the common law. Offences relating to cybercrime are primarily regulated under the Electronic Communications and Transactions Act 25 of 2002 ("**ECT Act**").

It has been recognised in South Africa that the current hybrid legal framework relating to cybercrimes (in particular the common law, which develops on a case-by-case basis) has not kept up with the dynamic nature of technology and international standards. Accordingly, in September 2015, the first draft Cybercrimes and Cybersecurity Bill ("**Cybercrimes Bill**") was published in the South African parliament for comment. The most recent version of the Cybercrimes Bill [B6 of 2017] has removed all references to Cybersecurity and was passed by the National Assembly on November 2018, the first parliamentary body of South Africa. It still must be passed by the second parliamentary body, the National Council of Provinces.

The Cybercrimes Bill, once effective, will, *inter alia*, consolidate and codify numerous existing offences relating to cybercrime as well as create a variety of new offences which do not currently exist in South African law. The Cybercrimes Bill also deals with penalties for such cybercrime offences, provides for the powers of investigation, search, access and seizure in relation to prosecution of such offences, and regulates jurisdiction of the courts.

It is important to note that once the Cybercrimes Bill is in effect, it will repeal the relevant provisions in the ECT Act relating to cybercrime offences. We therefore set out the current legal framework below, as well as how this may differ under the pending legislation.

Hacking (i.e. unauthorised access)

Yes. Hacking is recognised as an offence under section 86(1) of the ECT Act, which states that it is an offence to intentionally access or intercept data without the appropriate authority of permission to do so. This also applies to unauthorised interference with data as contained in section 86(2) of the ECT Act. Under the ECT Act, the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding 12 months.

Under the Cybercrimes Bill, the offence of hacking is more broadly defined as it encompasses the unlawful and intentional access to data, a computer program, a computer data storage medium, or a computer system (section 2(1)). Under the Cybercrimes Bill, the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding five years (or both).

Denial-of-service attacks

Yes. Section 86(5) of the ECT Act states that any person who commits any of the acts described in sections 86(1)–86(4) with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

For the sake of completeness:

- section 86(1) – see discussion above in relation to hacking;
- section 86(2) – criminalises the unlawful intentional interference with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective;
- section 86(3) – makes it an offence to unlawfully produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section; and
- section 86(4) – makes it an offence to utilise any device or computer program mentioned in section 86(3) in order to unlawfully overcome security measures designed to protect such data from access thereto.

Under the ECT Act, the maximum penalty for contravening section 86(5) is a fine (unspecified) or imprisonment for a period not exceeding five years.

Phishing

Yes. Phishing is recognised as an offence under section 87(2) of the ECT Act, which provides that a person who commits any of the acts described in sections 86(1)–86(5) for the purpose of obtaining an unlawful advantage by causing fake data to be produced with an intent that it would be considered or acted upon as if it were authentic is guilty of offence. The maximum penalty under the ECT Act is a fine (unspecified) or imprisonment for a period not exceeding five years.

Phishing can also be prosecuted under the common law offences of theft and fraud. The maximum penalty imposed would depend on which court hears the case (which would depend on a variety of

factors, the quantum of the claim being one). If the case is prosecuted in the Magistrate's Court, the court can impose a fine or imprisonment for a maximum period of 15 years in terms of its penal jurisdiction. If the case is heard in the High Court of South Africa, the court has wider discretion and may impose any fine or term of imprisonment which they deem appropriate in the circumstances.

Under the Cybercrimes Bill, there are separate offences for cyber fraud, cyber forgery and uttering and cyber extortion (sections 8, 9 and 10) which all attempt to deal with forms of phishing. A court which convicts a person of such an offence (where a penalty is not prescribed by any other law) can impose a sentence which the court deems appropriate and which is within that court's penal jurisdiction.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. See the discussion above in respect of denial-of-service attacks. Section 87(1) relating to computer-related extortion, fraud and forgery of the ECT Act is also relevant as it states that it is an offence to perform or threaten to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions.

Under the ECT Act, the maximum penalty imposed for contravention of section 86(4) or 87 is a fine (unspecified) or imprisonment for a period not exceeding five years.

Under the Cybercrimes Bill, there are separate offences for unlawful acts (in respect of software or hardware tools), as well as unlawful interference with data, a computer program, a computer data storage medium or a computer system (which is construed broadly enough to specifically include malware).

Under the Cybercrimes Bill, the maximum penalty for contravention of these sections is a fine (unspecified) or imprisonment for a period not exceeding 10 years (or both).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Yes. See the discussion above in respect of denial-of-service attacks. Section 86(3) of the ECT Act is relevant and the maximum penalty which can be imposed for contravention of section 86(3) is a fine or imprisonment for a period not exceeding 12 months.

Under the Cybercrimes Bill, it is an offence under section 4(1) to unlawfully and intentionally possess, manufacture, assemble, obtain, sell, purchase, make available or advertise any software or hardware tool for purposes of contravening certain other sections of the Cybercrimes Bill. The maximum penalty for contravention of this section is a fine (unspecified) or imprisonment for a period not exceeding 10 years (or both).

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Section 87 of the ECT Act (which deals with computer-related extortion, fraud and forgery) is relevant and criminalises the actions of a person who performs or threatens to perform any of the acts in section 86 for the purpose of obtaining any unlawful proprietary advantage, or obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic. If the offender uses an access device to breach certain security measures and then uses the data unlawfully, then the offender will have contravened section 87 and 86 of the ECT Act. As stated above, the maximum penalty imposed for contravention of section 87 is a fine (unspecified) or imprisonment for a period not exceeding five years.

Identity theft or fraud can also be prosecuted under the common law offence of "theft" or "fraud". The sentencing jurisdiction would operate the same as discussed above in relation to "phishing".

Depending on the nature of the offence, it may also be possible to prosecute identity theft or fraud as an infringement of copyright under copyright laws.

Under the Cybercrimes Bill, there are separate offences for cyber fraud, cyber forgery and uttering and cyber extortion (sections 8, 9 and 10) which are broad enough to cover identity theft or fraud. A court which convicts a person of such an offence (where a penalty is not prescribed by any other law) can impose a sentence which the court deems appropriate and which is within that court's penal jurisdiction.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Electronic theft may constitute an offence under section 86(1) of the ECT Act relating to unlawful access to data (see the discussion above in relation to hacking). It can also be prosecuted under the common law offence of theft.

Breach of confidence by a current/former employee would be actionable as a common law delict (tort), but not necessarily as a criminal offence.

With regards to criminal copyright infringement, the Copyright Act 98 of 1978 makes provision for criminal penalties, including a fine (a maximum of R5,000 per infringement) and/or imprisonment of up to three years for a first conviction. The maximum fine and/or imprisonment penalty for a second conviction is R10,000 and/or five years.

The Cybercrimes Bill also provides for theft of incorporeal property and states that the common law offence of theft must be interpreted so as not to exclude the theft of incorporeal property.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The ECT Act also criminalises attempting to commit any of the offences in the ECT Act or aiding and abetting those offences (section 88). The same penalties would apply as if the offence was successfully perpetrated.

Under the Cybercrimes Bill there are numerous new offences relating to "malicious communications". For example, it will be an offence to disseminate a data message which advocates, promotes or incites hate, discrimination or violence against a person or group of persons. The distribution of a data message of an intimate image without consent (often referred to as the "Revenge porn" offence) will also constitute an offence under the Cybercrimes Bill. The infringement of copyright (through the use of peer-to-peer file sharing) is also an offence under the Cybercrimes Bill.

Failure by an organisation to implement cybersecurity measures

Under the current legislative framework, there is no law which imposes a duty to implement specific cybersecurity measures on an organisation.

However, the Protection of Personal Information Act 4 of 2013 ("**POPI Act**"), which was promulgated in 2013 but which has not yet commenced, does contain obligations for responsible parties (data controllers) to implement reasonable technical and organisational measures to safeguard personal information in their possession or control against unauthorised access, which will likely involve cybersecurity measures. The POPI Act further imposes administrative fines as well as punitive penalties for infringement of its provisions.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Section 90 of the ECT Act lists the instances where South African courts will have extra-territorial jurisdiction in respect of cyber-related offences. This includes where the offence was committed in South Africa, where any preparatory act towards the offence was committed in South Africa, where the offence was committed by a citizen, resident or person carrying on business in South Africa or where the offence was committed on board any ship or aircraft registered in South Africa or on a voyage or flight to or from South Africa at the time the offence was committed.

Under the Cybercrimes Bill, the extraterritorial jurisdiction provisions are more extensive and even where an offence is committed outside of South Africa, a South African court will have jurisdiction if the person charged: is a citizen or ordinary resident of South Africa; was arrested in South Africa (or onboard a vessel registered in South Africa); or is a company or body of persons incorporated or registered in South Africa. An offence shall also be deemed to have been committed in South Africa under the Cybercrimes Bill if the act or commission affects or is intended to affect any person in South Africa or the perpetrator is found to be in South Africa; or if the perpetrator is not extradited by South Africa.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

There are no provisions in the ECT Act which deal with exceptions or mitigation of sentences. This would need to be considered by a court on a case-by-case basis.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Certain terrorism offences may arise in relation to cybersecurity or an Incident. South Africa does have in place legislation criminalising acts of terrorism, but it is broad enough to cover a multitude of scenarios. The offence of treason is a common law offence and is defined as "any conduct unlawfully committed by a person owing allegiance to a state with the intention of: (i) overthrowing the government of the Republic; (ii) coercing the government by violence into any action or inaction; (iii) violating, threatening or endangering the existence, independence or security of the Republic; and (iv) changing the constitutional structure of the Republic". The offence of treason may therefore also be construed broadly enough to include an Incident. We are not aware of any specific prosecutions in the cybersecurity context.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The legislative frameworks in South Africa that are relevant to cybersecurity are set out below:

- The right to privacy is enshrined in section 14 of the Constitution of South Africa, 1996 and states that "everyone has the right to privacy, which includes the right not to have their privacy of their communications infringed".
- In order to give effect to the right to privacy, the POPI Act was promulgated. The POPI Act is data protection legislation primarily modelled on the EU general data protection laws. Importantly, it establishes the Information Regulator and confers various powers, duties and functions including monitoring and enforcing compliance by public and private bodies and handling complaints in respect of contraventions of the POPI Act. It also establishes a comprehensive compliance framework and places cybersecurity obligations on responsible parties to secure the integrity and confidentiality of personal information in its possession or control by taking appropriate, reasonable technical and organisational measures to prevent unlawful access. The substantive provisions of the POPI Act are not yet in effect. The commencement date of the POPI Act is imminent.
- The ECT Act, as discussed in section 1 above, regulates electronic communications and transactions and is the primary legislation currently in force which criminalises cyber-related offences.
- The Cybercrimes Bill, as discussed in section 1 above, which is not yet in force, aims to provide for the criminalisation of a broad range of cyber-related crimes.
- The Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002 ("**RICA**") regulates the interception and monitoring of direct and indirect communications. RICA contains exceptions relating to where interception and monitoring takes place with the consent of the parties involved or where it is carried out by law enforcement personnel.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

There is no legislation in force which specifically relates to cybersecurity requirements applicable to critical infrastructure at present. The latest version of Cybercrimes Bill that was passed by the National Assembly has removed references to national critical information infrastructures which were referenced in the previous version of the Cybercrimes Bill.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Once the POPI Act comes into operation, the responsible party (similar to data controller) will be required to take appropriate reasonable technical and organisational measures to prevent unlawful access to personal information in its possession or control (section 19). This obligation will include taking measures to monitor, detect, prevent or mitigate Incidents. As the POPI Act is not yet in effect, the Information Regulator has not published any regulations or guidance on what measures are required to be taken.

The King IV Report on Corporate Governance for South Africa – 2016 ("**King IV**") is a set of voluntary principles in the area of corporate governance. Companies listed on the Johannesburg Stock Exchange are, however, required to comply with King IV by law. In particular, King IV has a specific focus on the oversight of information and technology management. The board of the company is specifically tasked to make sure it proactively monitors cyber Incidents and ensure that it has systems and processes in place from a cybersecurity perspective.

The Cybercrimes Bill also places obligations on electronic communication service providers and financial institutions which become aware that its electronic communications network is being used to commit an offence to immediately report the matter in the prescribed manner to the South African Police Services and preserve all information/evidence that will be relevant to the investigation of the offence.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Not at this stage, as the provisions of the POPI Act are not yet in force. The Cybercrimes Bill has also not been promulgated into law yet.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under current law, there is no duty to report Incidents to a regulatory or other authority.

Once the POPI Act comes into operation, section 22 provides that responsible parties must inform both the Information Regulator and the affected data subjects (unless the identity of such data subjects cannot be established) in writing as soon as reasonably possible that there is a breach or suspected breach – where there are reasonable grounds to believe that personal information of a data subject has been accessed or acquired by an unauthorised person. The notification must contain sufficient information to enable the data subject to take protective measures against potential consequences of the Incident. The Information Regulator may also direct the responsible party to publicise such Incident.

Under the Cybercrimes Bill, an electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of an offence must, without undue delay and not later than 72 hours after having become aware of the offence, report the offence in the prescribed form to the South African Police Services and preserve any evidence which may be of assistance to law enforcement agencies in investigating the offence.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There is no prohibition under current laws which would prevent organisations from voluntarily sharing information relating to Incidents with regulatory authorities in South Africa or outside of South Africa, provided such information is not subject to confidentiality restrictions, deemed classified or otherwise restricted.

The POPI Act is, however, not yet in operation, so the Information Regulator has not published any regulations or guidance notes on this issue. There are regulations that were issued on 14 December 2018 that, like the POPI Act, are not yet in in operation. However, these do not deal specifically with the reporting of Incidents.

The Cybercrimes Bill does provide for mutual assistance and sharing of information relating to Incidents to law enforcement agencies of foreign states where the disclosure of such information may assist the foreign state in carrying out investigations or may lead to co-operation with the foreign state to carry out an investigation. It also provides for the process for foreign requests for assistance and co-operation.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, see the answer to question 2.5 above.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

At this stage, the reporting and notification obligation under the POPI Act will only apply to the extent that the Incident involves personal information. IP addresses and email addresses may constitute personal information. Once the POPI Act comes into operation, the Information Regulator may also publish further regulations or exemptions on this issue.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Under the POPI Act, the Information Regulator (http://www.justice.gov.za/inforeg/) is responsible for enforcing the requirements.

Under the Cybercrimes Bill, the following authorities are relevant:

- the South African Police Services;
- the State Security Agency; and
- the National Prosecuting Authority.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The Information Regulator may impose administrative fines on responsible parties to a maximum of R10 million. Depending on the offence, the POPI Act also provides for fines and imprisonment not exceeding 10 years.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The POPI Act and Cybercrimes Bill are not yet in force and accordingly no enforcement action has been taken. Once the POPI Act comes into force, there will be a grace period of one year (which may be extended for up to three years) for responsible parties to comply with the provisions of the POPI Act.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Currently there is no legislation restricting the use of beacons; however, once POPI comes into effect, IP Addresses are likely to be considered personal information (like they are under GDPR). Thus the processing of personal information through the use of beacons would only be authorised if it is processed in accordance with one of the lawful grounds of processing such as consent or in terms of a contract and this would have to be in terms of a legitimate purpose.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There are no laws under South African law that we are aware of that would restrict a company from using honeypots in order to better protect their network provided that if the use of honeypots resulted in the processing of personal information this was done so in accordance with the provisions of the POPI Act, once the Act comes into full operation. This would include that the processing of personal information must be in accordance with one of the lawful grounds of processing such as consent of the data subject.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

There are no laws under South African law that we are aware of that would restrict a company from using sinkholes in order to better protect their network provided that if the use of sinkholes resulted in the collection of personal information, this was done so in accordance with the provisions of the POPI Act once it comes into full force and effect. One of the lawful grounds under POPI for the processing of personal information is legitimate interest of the responsible party (data controller). This ground is dependent on the circumstances, likely to be a good ground for justifying the use of sinkholes (where these process personal information).

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

While there are no strict legal requirements under Applicable Laws which require different business sectors to address cybersecurity differently, certain sectors such as financial services (in particular banks and insurers who hold licences) tend to be more incentivised to avoid the cost and reputational impact of Incidents. As the POPI Act has been promulgated (but not yet effective) for a few years now, many organisations' cybersecurity practice is driven not just by "compliance" but also promoting good business practices. Once the POPI Act comes into force, the Information Regulator may publish industry-specific Codes of Conduct for different business sectors.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Cybercrimes Bill will place obligations on electronic communication service providers (which includes financial institutions and any entity or person who is declared by the Minister of State Security to own or control a critical information structure) which become aware that its electronic communications network is being used to commit an offence to immediately report the matter in the prescribed manner to the South African Police Services and preserve all information/evidence that will be relevant to the investigation of the offence.

The South African Reserve Bank's directive on cloud computing and data offshoring, effective from October 2018 (and which applies to all banks) imposes obligations on banks to implement a formally defined and board approved data strategy and data governance framework. The Prudential Authority, which regulates insurers and financial service providers, also issued a directive which contains similar requirements.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

See the discussion above under question 2.3 relating to King IV, which places obligations on the board of directors of the company to make sure it proactively monitors cyber Incidents and ensure that it has systems and processes in place from a cybersecurity perspective.

While the principles in King IV are voluntary (except for listed companies), failure by a company to prevent, mitigate, manage or

respond to an Incident amount to a breach of directors' duties both under the common law and the Companies Act 71 of 2008 ("**Companies Act**").

Under the common law, a breach of fiduciary duties may apply, and the director can be held liable for any losses, damages or costs. Section 76 of the Companies Act sets out standards of directors conduct and that a director must always act in good faith, for a proper purpose, in the best interest of the company and with a degree of reasonable care, skill and diligence. Failure to prevent, mitigate, manage or respond to an Incident may amount to a breach of directors' duties under the Companies Act.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

No, there are no Applicable Laws which require companies to satisfy any of the specific requirements above. However, see the discussion above under question 2.3 relating to King IV, which places obligations on the board of directors of the company to make sure it proactively monitors cyber Incidents and ensures that it has systems and processes in place from a cybersecurity perspective.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no additional requirements other than what has been set out under questions 2.5 and 2.7 above.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

There are a variety of civil actions which may be brought in relation to an Incident; the most relevant would probably be a claim for compensation (or damages) under a delictual action (*action lex aquila* – similar to tort). The claimant would need to claim against the organisation or individual which caused the Incident. In order to be entitled to compensation in damages, the claimant would need to prove: (i) a wrongful act or omission (i.e. the Incident); (ii) caused by negligence/fault/breach of duty of care; and (iii) actual monetary loss on the part of the claimant.

It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract where the particular Incident constituted a breach of contract between the parties.

Section 99 of the POPI Act also provides for civil remedies in terms of which a data subject or the Information Regulator may institute a civil action for damages against a responsible party for breach of the provisions of the POPI Act (as referred to in section 73) whether or not there is intent or negligence on the part of the responsible party.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

As far as we are aware, there have not been any specific cases in relation to Incidents brought in South Africa.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes; see the answer to question 5.1 above.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, although this is still relatively new in South Africa and the market has been slow to take up cyber-risk insurance cover (because South Africa has been slow in promulgating its data protection and cybersecurity legislation). Typically, this sort of insurance would cover business interruption, system failures, cyber extortion, etc.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limits on what the insurance policy can cover. The general rules of insurance would apply.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No, there is no legislation which requires the monitoring of employees for the purposes of preventing, detecting, mitigating and responding to Incidents. Monitoring of employees' use of email and internet access, for example, will involve the processing of personal information and therefore the POPI Act (once effective) will apply.

RICA regulates the interception and monitoring of direct and indirect communications. RICA contains exceptions relating to where interception and monitoring takes place with the consent of the parties involved or where it is carried out by law enforcement personnel.

While there are no specific laws which place a duty on employees to report cyber risks, security flaws, Incidents or potential Incidents to their employers, once the POPI Act comes into effect it is likely that the employee (in the capacity of an operator) will have to notify the responsible party immediately if there are reasonable grounds to

believe that the personal information of a data subject has been accessed by an unauthorised person.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws which may prevent or limit the reporting of Incidents by an employee. For whistle-blowers, the employee would need to satisfy the whistleblowing provisions in the Protected Disclosures Act 26 of 2000, one of which is that the subject matter of the disclosure falls into one or more categories. The categories include criminal offences and breach of a legal obligation, which may be appropriate for Incidents, although may not be wide enough to cover security flaws or mere risks.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Currently, the South African Police Services has general law enforcement and investigatory powers to investigate an Incident. The Criminal Procedure Act 51 of 1977 sets out the procedure to be followed by the South African Police Services when investigating a criminal offence.

The POPI Act grants broad powers to the Information Regulator to, *inter alia*, commence an investigation at their own initiative, summon people to appear before it and give evidence, enter and search any premises, conduct interviews, carry out enquiries as the Information regulator sees fit and refer complaints to other bodies.

The Cybercrimes Bill establishes procedures which specifically cater for the investigation of cyber-related offences. The Cybercrimes Bill confers extensive powers to law enforcement authorities and other investigators in respect of access, search and seizure of articles involved in the commission of an offence. Section 52 also provides that the National Commissioner of the South African Police Service ("**SAPS**") must establish or designate an office known as the designated Point of Contact within the existing structures of the South African Police Service and mutual legal assistance in the arena of cybercrimes (different law enforcement agencies working together to facilitate enforcement and compliance). The Cybercrimes Bill also authorises the National Director of Public Prosecutions to submit the request for mutual assistance and co-operation relating to the investigation and prosecution of cyber-related offences with foreign states, together with his or her recommendations, to the Cabinet member responsible for the administration of justice, for his or her approval.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements under the Applicable Laws.

Fatima Ameer-Mia is a Director in the Technology, Media & Telecommunications practice in Cape Town. Fatima specialises in commercial, information technology, intellectual property and data protection law. She also has a special interest in the fields of e-commerce and matters relating to cybercrime and information security. Fatima advises clients, both locally and internationally, in various sectors on their commercial and technology arrangements, including outsourcing, software licensing and development and systems integration.
She regularly advises on data protection and information security, including providing training, seminars, risk assessments and governance frameworks on cybersecurity and data protection laws.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town, 8001
South Africa

Tel: +27 21 481 6300
Email: fatima.ameermia@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Christoff Pienaar is Director and National Head of our Technology, Media & Telecommunications practice. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions.
Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town, 8001
South Africa

Tel: +27 21 481 6300
Fax: +27 21 481 6388
Email: christoff.pienaar@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Nikita Kekana is an Associate in our Technology, Media & Telecommunications practice. Nikita specialises in privacy, data protection law, commercial, information technology and intellectual property law. Nikita also has a keen interest in artificial intelligence law. Nikita completed her LL.B. at the University of Cape Town in 2016.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town, 8001
South Africa

Tel: +27 21 481 6300
Fax: +27 21 481 6388
Email: nikita.kekana@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Spain

SAMANIEGO LAW

Javier Fernández-Samaniego

Gonzalo Hierro Viéitez

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Article 197 *bis* of the Spanish Criminal Code (hereinafter, "**SCrC**") establishes that those, who by any means, without being authorised, breach the security measures and access or facilitate access to an information system, or part of it, or stays in it against the will of whoever has the legitimate right to exclude access, may be punished with up to two years in prison.

Denial-of-service attacks
Denial-of-service attacks ("**DOS**" attacks) are foreseen in Article 264 *bis* SCrC, which holds that causing unauthorised hinderance or interruptions to an informatic system is punishable by up to three years in prison. Article 264.2 SCrC enumerates a series of aggravated cases where the prison term may be as high as five years' imprisonment and a fine.

Phishing
Phishing is foreseen in Article 248.2 SCrC, which identifies phishing as "those who, for profit and using any kind of informatic manipulation –or similar– obtain a non-consensual transfer of assets to the detriment of another". The maximum penalty is three years in prison.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Article 264.1 SCrC holds that any unauthorised erasure, damage, deterioration, alteration or deletion of computer data, software or electronic documents of others, or making it inaccessible, where the result produced is serious, shall be punished with imprisonment of up to a maximum of three years. Article 264.2 SCrC enumerates a series of aggravated cases where the prison term may be as high as five years and a fine.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The possession or use of hardware, software or other tools used to commit cybercrime, as well as their import, production or, by any means, supply to third parties is foreseen in Article 197 *ter* SCrC. The penalty may be a maximum of two years in prison or a fine.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft is not expressly foreseen in the Spanish Criminal Code. However, some of the most common crimes associated with identity theft or identity fraud, such as those in connection with access devices, e.g. swindling and fraud, are found in Articles 248 *et seq.* and 436 *et seq.*, respectively.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Article 199 SCrC holds that whoever reveals other people's secrets, which he is aware of by reason of his trade or his employment relationships, shall be punished by imprisonment of up to three years and receive a fine.

Article 270 SCrC, which foresees criminal copyright infringement, dictates that those who, in order to obtain a direct or indirect economic benefit to the detriment of a third party, reproduce, plagiarise, distribute, publicly communicate or exploit, in whole or in part, a literary, artistic or scientific work without the authorisation of the holders of the corresponding intellectual property rights, or their assignees, may be punished with up to four years in prison and a fine.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Article 197 SCrC foresees that the interception of telecommunications via listening, transmitting, recording and/or reproduction devices shall be punishable by imprisonment of up to four years and receive a fine.

Failure by an organisation to implement cybersecurity measures
No, failure to implement appropriate cybersecurity measures is not foreseen by the SCrC. However, under the GDPR, organisations may be fined if they do not have in place the appropriate measures to prevent data breaches, taking into account the most recent technical developments, risks, the nature of personal data being processed and the damages to the rights and freedom of the data subject.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The extraterritorial application of the SCrC is foreseen in Article 23.2 of the Organic Law 6/1985, of 1 July, on Judicial Power. Article 23.2 holds that Spanish courts will know of crimes committed outside of the Spanish territory as long as the authors are Spanish or they obtain the Spanish nationality, and the following three requisites are met:

i. that the crime is punishable at the place of execution (unless, under an international treaty or a normative act of an international Organisation to which Spain is a party, such a requirement is not necessary);

ii. that the aggrieved person or the Public Prosecutor's Office files before the Spanish courts; and
iii. that the offender has not been acquitted, pardoned or sentenced abroad, or, in the latter case, has not served his sentence.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Besides the mitigating circumstances (Article 21) and the exceptions (Articles 19 and 20) under the general rules of the SCrC, we must highlight, in relation to companies, that an effectively implemented compliance programme may exempt a company from liability.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Article 573.2 SCrC holds that the crimes established under Articles 197 *bis*, 197 *ter* and 264 through 264 *quater* are considered terrorism offences when done with any of the following ends:
i. subvert the constitutional order, supress or destabilise political institutions or economic or social structures of the State or compel the public authorities to perform an act, or to refrain from doing so;
ii. alter public peace;
iii. destabilise the functioning of an international organisation; or
iv. provoke a state of terror in the population or a part of it.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The following European Union ("**EU**") Regulations have a direct effect in Spain:
i. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"); and
ii. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification ("**Cybersecurity Act**").

Please find the link to the Cybersecurity Code, published by the Spanish Official Gazette editorial, listing all the Applicable Laws related to cybersecurity. Due to the complexity and length of the Spanish regulation on cybersecurity, encompassing over 50 different Applicable Laws, we list below the most relevant ones:
i. Law 36/2015, of 28 September 2015, on National Security;
ii. Law 8/2011, of 28 April 2011, on Measures for the Protection of Critical Infrastructure incorporating Directive 2008/114/EC;
iii. Royal Decree-Law 12/2018, of 7 September 2018 ("**Royal Decree-Law 12/2018**"), incorporating Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union ("**NIS Directive**");
iv. Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce, incorporating E-Commerce Directive 2000/31/EC;
v. Law 59/2003, of 19 December, on the Electronic Signature, incorporating Directive 1999/93/EC;
vi. the General Telecommunications Law 9/2014, of 9 May;
vii. Organic Law 10/1995, of 23 November, on the Criminal Code; and
viii. Organic Law 3/2018, of 5 December on Data Protection and the Guarantee of Digital Rights ("**LOPDGDD**" as per its Spanish initials), which develops the GDPR in Spain.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Article 13 of Law 8/2011 of 28 April on Measures for the Protection of Critical Infrastructures mentions that those who operate Critical Infrastructures must elaborate security plans while Article 16 requires them to appoint a Security and Liaison Officer.

The Regulation on the Protection of Critical Infrastructures, approved by the Royal Decree-Law 704/2001 of 20 May, has developed, concreted and expanded the aspects referred to in Law 8/2011. Articles 22.4 and 25.5 of the Regulation established that the State Secretary of Security would indicate the minimum contents of the Security Plans of the Operator and of the Specific Security Plans mentioned in Article 14 of Law 8/2011. Said minimum contents are described in the Resolution of 8 September 2015 of the State Secretary of Security ("**Resolution**").

The Resolution does not impose any specific cybersecurity requirements. Its main purpose is to establish a methodology to elaborate and design the Security Plans of the Operator (Annex I) and the Specific Security Plans (Annex II).

Royal Decree-Law 12/2018 does not impose harsher security requirements than the NIS Directive, however, it applies not only to Critical Infrastructures but also to Digital Service Providers.

There is a project of a regulation that will further develop the content of Royal Decree-Law 12/2018, which is in the stage of public consultation until 6 September, 2019.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Pursuant to Articles 24 and 25 GDPR, the controller and the processor must implement appropriate technical and organisational measures, such as pseudonymisation, to ensure a level of security appropriate to the identified risk.

Article 28 LOPDGDD references Articles 24 and 25 GDPR in order to determine the appropriate technical and organisational measures to be implemented.

On a side note, the authors recommend to visit the webpage of the National Institute of Cybersecurity of Spain (*Instituto Nacional de Ciberseguridad de España*; "**INCIBE**" as per its Spanish initials) which has a help centre on cybersecurity, available for both companies and individuals, that may be reached by calling the Spanish free toll

number 900 116 117. Furthermore, they periodically publish a Bulletin on cybersecurity.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

The risk of conflicts of laws is minimised due to the harmonisation of Applicable Laws at EU level.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Unlike Incidents in Critical Infrastructures or Digital Service Providers where Royal Decree-Law 12/2018 requires, in the event of an Incident that might have significant disturbing effects, that the competent authority be notified (a notification may also be made even if the Incident has not yet produced an adverse effect), organisations are not required to report information related to Incidents or potential Incidents unless the Incident relates to personal data. If such an Incident has an impact on the data subject's rights, the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*; "**Spanish DPA**") should be notified. The notification shall at least:

i. describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
ii. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
iii. describe the likely consequences of the personal data breach; and
iv. describe the measures to be taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations are permitted to voluntarily share information related to Incidents and encouraged to do so with the Computer Security Response Team of INCIBE.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

When personally identifiable information of an individual is involved in an Incident, under the GDPR, the controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach, as well as recommendations to mitigate potential adverse effects.

For information purposes, the Spanish DPA has developed a Data Breach Notification form for controllers (Article 33 GDPR) through its online portal.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

None of these cases would change the responses to questions 2.5 to 2.7.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regarding Critical Infrastructures, the relevant authority regarding Incidents is the National Centre for the Protection of Infrastructures and Cybersecurity (*Centro Nacional de Protección de Infraestructuras y Ciberseguridad*), whose email for information purposes is ses.cnpic-buzon@interior.es and for Incident-reporting purposes is incidencias.occ@interior.es.

Regarding Digital Service Providers, the relevant authority regarding Incidents depends on whether the Digital Service Provider is from the public or private sector. In the private sector, the relevant authority is the State Secretary for Digital Progress (*Secretaría de Estado para el Avance Digital*) under the Ministry of Economy, whose telephone number for information purposes is +34 912 582 852. In the public sector, the relevant authority is the National Cryptologic Centre (*Centro Criptológico Nacional*), whose email for information purposes is info@cnn-cert.cni.es and for Incident-reporting purposes is incidentes@cnn-cert.cni.es.

The relevant authority regarding Incidents with an impact on personal data is the Spanish DPA (*Agencia Española de Protección de Datos*), with headquarters in C/ Jorge Juan, 6, 28001 Madrid, telephone number +34 912 663 517.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Under the GDPR, depending on the nature of the infringement, the administrative fine may amount up to 10,000,000 EUR or 2% of the company's worldwide turnover, and 20,000,000 EUR or 4% of the company's worldwide turnover.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There have yet to be any enforcement actions related to the lack of reporting of Incidents imposing fines; however, there have been several warnings by the Spanish DPA.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Yes, the use of beacons is allowed.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Yes, the use of honeypots is allowed.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Due to its direct consequences, sinkholing is usually done in special conditions by trusted third parties with the involvement of law enforcement authorities.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The measures to be implemented are stronger in some business areas, particularly for Critical Infrastructures and Digital Service Providers, which must comply with Royal Decree-Law 12/2018. Companies who host personal health data must also implement stronger security measures as foreseen in the 17th additional provision of the LOPDGDD. With regards to the telecommunications sector, Article 44 of the General Telecommunications Law 9/2014, of 9 May, establishes that network operators and operators of electronic communications shall adequately manage security risks that may affect their network and services in order to ensure an adequate level of security, and avoid or minimise the impact that Incidents may have on users and interconnected networks.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

As mentioned above, the NIS Directive has been implemented in Spain by Royal Decree-Law 12/2018 which regulates, among others, the Critical Infrastructures and Digital Service Providers of these two sectors.

In relation to cybersecurity in the financial services sector, entities subject to the GDPR and the Directive (EU) 2015/2366 (the PSD2 Directive) will have to follow two notification processes in case they suffer a major Incident involving personal data. Furthermore, the National Securities Market Commission (*Comisión Nacional del Mercado de Valores*) is looking to regulate, in the short term, the cybersecurity measures which fund managers should implement to control the technological risks associated with their activities.

Regarding the requirements of the telecommunications sector, besides those established in Royal Decree-Law 12/2018, under Article 12 *bis* of Law 34/2002 of 11 July on Information Society Services and Electronic Commerce, Internet service providers have a series of obligations to inform its users, among others, of the different ways to implement and/or increase security measures. In addition, the ninth additional provision of Law 34/2002 holds that information society service providers, domain name registrations and registrars established in Spain are required to collaborate with the competent Computer Security Response Team in resolving Incidents affecting the Internet. Furthermore, they are required to follow specific recommendations on the management of cybersecurity Incidents, which will be developed via codes of conduct (which have yet to be developed). Also, see the answer to question 3.1.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Such a failure may lead to a breach of the directors' duties, as Article 225 of the Spanish Companies Act, concerning duty of care, holds that directors shall perform the duties imposed by laws and statutes with the diligence of an ordained businessman, taking into account the nature of the position and duties assigned. In addition, directors shall have the appropriate dedication and take precise measures for the good direction and control of the company. The Spanish Companies Act, in case of a breach, allows for the director to be liable for damages caused by acts or omissions.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Currently, there is no obligation to designate a CISO, establish a written Incident response plan or policy, conduct periodic risk assessments or perform penetration tests or vulnerability assessments. However, in order to comply with Article 32 GDPR, such measures may be required in order to ensure appropriate security measures. In this sense, security measures must be implemented with consideration given to the level of associated risk. Therefore,

the implementation of these security measures must be assessed on a case-by-case basis.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

In connection with the directors' duty of care (see the answer to question 4.1), under the Spanish Companies Act, the shareholders of a company have the right to be informed when the topic is included in the agenda of the shareholders' meeting.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, there are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

A civil liability action for damages may be brought under Article 1902 of the Spanish Civil Code, which holds that the person who, as a result of an action or omission, causes damage to another by his fault or negligence shall be obliged to repair the damage caused. Three elements are necessary to establish liability:

i. a fault;
ii. a damage; and
iii. a causal link between i. and ii.

Furthermore, under Article 79 GDPR, a civil action may be brought in the event of an Incident if the controller or processor has not complied with its provisions. In addition, the GDPR foresees the possibility to initiate "European-style" class actions related to data protection matters.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There have been many cases brought before the Spanish courts in relation to Incidents. As an example, a bank was sentenced to pay plaintiffs 139,257.04 EUR, amounting to the value stolen, by the Provincial Court of Barcelona in its decision of 22 January 2019 after suffering a phishing attack. However, due to the elusiveness of the authors of cybercrimes, many go unpunished, such as the case of the ransomware Wannacry which affected, among others, Telefónica.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

In order to exclude liability under the accountability principle stated by the GDPR and the NIS Directive, companies should be in a position to provide sound evidence that they have implemented the appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, under Law 50/1980, of 8 October, on Insurance Contracts ("**Law on Insurance Contracts**"), insurance against Incidents is permitted. With the number of cyberattacks on the rise, the Spanish cyber-insurance trend is growing rapidly with many major providers offering cyber-insurance in order to cope with these new risks.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

The Law on Insurance Contracts imposes two limitations:

i. the insurer does not cover loss or damage resulting from the insured's intentional or wilful misconduct; and
ii. the insurer does not cover the payment of any administrative or judicial sanction, neither any cost derived from it.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

For the monitorisation of employees and the reporting of Incidents, three requirements should be met:

i. a previous communication where the employees are told that the company's computer is limited to professional use;
ii. that any breach of i. may be sanctioned; and
iii. that i. and ii. be proportional.

Regarding the reporting by employees to their employer, the designated data protection officer ("**DPO**") has the task of monitoring compliance with the GDPR, which includes the obligation of reporting certain Incidents. Besides the DPO, no other employee has a legal obligation to report a cyber risk, security flaw, Incident or potential Incident unless it is established by the employer through internal regulations.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are no Applicable Laws that may prohibit or limit reporting.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Cybersecurity is classified as of special interest to national security by Article 10 of Law 36/2015, of 28 September, on National Security.

The laws that may be relied upon to investigate an Incident are, besides those already mentioned in question 2.1, the following:

i. Organic Law 4/2015, of 30 March, on the Protection of the Safety of Citizens;
ii. Law 5/2014, of 4 April, on Private Security; and
iii. Royal Decree-Law of 14 September 1882 approving the Criminal Procedure Law which foresees technology-related investigation measures such as searches on mass storage devices and remote searches on computer systems, among others.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, in Spain there is no Applicable Law that requires organisations to implement backdoors or to provide encryption keys, as one of the basic principles of Criminal Law is the privilege against self-incrimination and the presumption of innocence.

Javier Fernández-Samaniego is the Managing Director of SAMANIEGO LAW and his international practice focuses mainly on commercial/IT disputes (litigation, arbitration and ADR) and negotiations and major tech & privacy projects (new cloud and big data business models, outsourcing transactions, data protection review programmes, etc.). Javier has vast experience assisting European clients in their expansion into Latin America and US clients in their European expansion. Javier is Senior Fellow at Florida International University, developing its Latin Atlantic Tech Law Collaborative. Before launching Samaniego Law in 2017, Javier was founding and managing partner of the Spanish office of Bird & Bird and head of its Commercial, DR and IT teams for over a decade. Before that Javier worked at Linklaters, Cuatrecasas and CDTI (Spanish Centre for the Development of Industrial Technology).

SAMANIEGO LAW
c/ Serrano 16, 6 D
28001 Madrid
Spain

Tel: +34 910 66 41 06
Email: javier.samaniego@samaniegolaw.com
URL: www.samaniegolaw.com

Gonzalo Hierro Viéitez focuses his practice on transactional and contentious IT law. Before joining SAMANIEGO LAW, he was an associate in the Commercial & IT and Dispute Resolution Groups of Bird & Bird based in Madrid. Prior to that, he was an intern at Cuatrecasas NYC office in its M&A group and at Ashurst London office in its international arbitration group. Gonzalo holds a law degree from Rey Juan Carlos University, a double Master's degree from Carlos III University and ISDE in the Practice of Law and in International Law, Foreign Trade and International Relations, respectively, as well as a dual concentration LL.M. from Fordham University in Banking, Corporate and Finance (awarded *magna cum laude*) and in Information Technology Law. He is licensed to practise law in Spain, admitted to the Madrid Bar and has passed the July 2018 New York Bar Exam.

SAMANIEGO LAW
c/ Serrano 16, 6 D
28001 Madrid
Spain

Tel: +34 910 66 41 06
Email: gonzalo.hierro@samaniegolaw.com
URL: www.samaniegolaw.com

SAMANIEGO LAW is an Ibero-American alternative law firm specialising in IT law and dispute resolution with offices in Madrid and Miami. The firm is a hybrid that combines an international commercial law firm, a legal strategy consultancy firm and a sophisticated solutions platform. The team comprises lawyers and strategic and IT consultants, with support from a long-standing network of trusted professionals and legal interim managers. The firm boasts a simple and flexible organisational structure with smart use of technology, allowing it to offer clients a significant reduction in fees. The firm's clients are typically technology companies and providers of digital transformation solutions, as well as organisations that want to reinvent their business. The firm has a clear focus on the Latin Atlantic region and regularly advises American companies expanding into Europe and, *vice versa*, European companies expanding into the Americas.

www.samaniegolaw.com

Sweden

Anders Hellström

Erik Myrberg

Synch Advokat

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking (intentionally giving oneself unauthorised access to electronic information) is considered a data breach (Sw. *Dataintrång*) according to the Swedish Penal Code. The penalty for data breach is either a fine or a maximum of two years in prison. Serious offences of data breach are punishable by at least six months in prison but no more than six years.

The Swedish Supreme Court found a police officer guilty of data breach and sentenced him to a fine. The police officer used the internal IT system of the Swedish police to search for himself with the purpose of finding out whether any information was registered about him or not. The police officer had proper access to the systems for other purposes, but no authorisation to carry out the abovementioned search.

Denial-of-service attacks
According to the Swedish Penal Code, denial-of-service attacks (intentionally causing severe disturbance or hindering access to electronic information) is considered a data breach. The penalty for data breach is either a fine or a maximum of two years in prison. Serious offences of data breach are punishable by at least six months in prison but no more than six years.

The Swedish Court of Appeal sentenced a man to imprisonment for shutting down the websites of two major banks in Sweden for a duration of 45 minutes by using denial-of-service attacks. With regards to the offenders age, the imprisonment was changed to a conditional sentence.

Phishing
Phishing is covered by the provision on fraud in the Swedish Penal Code. The penalty for fraud is either a fine or a maximum of two years in prison. Serious offences of fraud are punishable by at least six months in prison but no more than six years.

The District Court of Malmö sentenced four people to imprisonment for sending emails imitating email communication from different banks. The emails caused some of the recipients to provide their personal payment information to the fraudsters in the belief that they communicated with the banks.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The Swedish Court of Appeal has ruled that unauthorised installations of software on an IT system is not a crime in itself but if the installation is harming or disturbing electronic information on, e.g., the computer on which it is installed, the prerequisites for data breach are met according to the Swedish Penal Code. The penalty for data breach is either a fine or a maximum of two years in prison. Serious offences of data breach are punishable by at least six months in prison but no more than six years.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The mere possession of hacking tools is not criminalised in Sweden but, where it can be shown that this would constitute preparation for data breach, it is considered a crime according to the Swedish Penal Code. The penalty for data breach is a fine or a maximum of two years in prison. Serious offences of preparation for data breach is punishable by at least six months in prison but no more than six years.

The Swedish Copyright Act prohibits the use, development, marketing and possession of technical instruments, components and services whose purpose is to gain unauthorised access to material protected by copyright. The penalty for violation of the abovementioned prohibition is a fine or a maximum of two years in prison.

Furthermore, the Swedish Act on Decoding prohibits the use, development, marketing and possession of hardware and software which is designed to be used for decoding the services defined in the abovementioned law (e.g. radio and TV broadcasting to the public). The penalty for breach of the Swedish Act on Decoding is a fine or a maximum of two years in prison.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes, identity theft and identity fraud are crimes according to the Swedish Penal Code. The penalty for identity theft and identity fraud is either a fine or a maximum of two years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Copyright infringement is regulated by the Swedish Copyright Act. The penalty for copyright infringement is either a fine or a maximum of two years in prison. The Swedish Supreme Court sentenced a man to prison (which later was changed to a fine) for making available 125 movies and TV-series to the public without the rightsholders' permission. The movies and TV-series were shared online through torrent-files.

It is not a criminal offence if a current or former employee is disclosing information subject to confidentiality which is imposed

on the employee by a contract between him/her and the employer but it can be punishable to, e.g., make trade secrets public, according to the Swedish Trade Secrets Act (Sw. *Lag om företagshemligheter*). The penalty for violating the Swedish Trade Secrets Act is to pay damages.

Certain categories of professions are subject to statutory confidentiality (e.g. lawyers and doctors). For example, a lawyer who is a member of the Swedish Bar Association is not allowed to disclose information regarding his clients according to the Swedish Code of Judicial Procedure. According to the Swedish Penal Code, disclosure of information subject to statutory confidentiality is punishable by a fine or a maximum of one year in prison.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Further to what is mentioned above, it can be noted that destroying or causing damage to physical equipment such as computers, servers and transmitters would in general be considered acts of damage to property (Sw. *Skadegörelse*), which is criminalised under the Swedish Penal Code and can result in a maximum of two years of imprisonment.

Destroying or causing damage to equipment of importance to national security, the legal system, public order or administration, may be considered sabotage according to the Swedish Penal Code. The penalty for sabotage is either a fine or a maximum of two years in prison. Serious offences are punishable by at least six months in prison but no longer than six years.

Failure by an organisation to implement cybersecurity measures

Applicable law regarding critical infrastructure, data protection and telecom contains provisions addressing the failure to implement security measures regarding processing of personal data and keeping IT systems secured. Such failure is usually sanctioned by a regulatory fine.

In the context of criminal law, the Swedish Penal Code does not criminalise the failure by an organisation to implement cybersecurity measures.

1.2 Do any of the above-mentioned offences have extraterritorial application?

First, it shall be noted that a requirement of double criminality applies in Sweden. In order for a crime committed abroad to be punishable in Sweden, it needs to be criminalised also in the country where it is perpetrated (with some exceptions). Consequently, according to the Swedish Penal Code, extraterritorial application regarding data breach applies if the offence is carried out by a Swedish citizen or a foreigner living in Sweden and the act is also criminalised in the country where it is carried out. Swedish law also applies if a crime that can be punishable by more than six months in prison has been carried out abroad by a foreigner who does not live in Sweden but is located in the country.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

According to the Swedish Penal Code, a penalty can be mitigated if the offender can prove that he/she tried to reduce or hinder the offence.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Hacking can be considered a terrorism offence if the act has the potential to cause severe damage to a country or an IGO and the intention of the act is to: (i) create serious fear amongst a group of people; (ii) force a government or an IGO to act in a way preferred to the one carrying out the hacking; or (iii) cause serious destabilisation or destroy constitutional, political, economic or social structures of a state or an IGO. The penalty for terrorism is a minimum of two years in prison with the maximum of a life-long sentence.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- The processing of personal data is regulated by the EU General Data Protection Regulation (GDPR).
- The processing of personal data by governmental agency's regarding prevention, investigation, prosecution and the like is regulated by the Swedish Act on Processing of Personal Data Relating to Criminal Offences (Sw. *Brottsdatalagen*).
- Criminal offences (e.g. hacking, denial-of-service attacks, phishing, etc.) is subject to the Swedish Penal Code (Sw. *Brottsbalken*).
- Copyright infringement is governed by the Swedish Copyright Act (Sw. *Lag om upphovsrätt till litterära och konstnärliga verk*).
- Decoding of radio and TV is regulated by the Swedish Act on Decoding (Sw. *Avkodningslagen*).
- Terrorism offences in the context of cybersecurity is regulated by the Swedish Act on Criminal Responsibility for Terrorist Offences (Sw. *Lag om straff för terroristbrott*).
- The Swedish Act on Electronic Communication regulate the providers of electronic communications (Sw. *Lag om elektronisk kommunikation*).
- The Directive on Security of Network and Information Systems (NIS) is implemented in Sweden as The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services and regulate providers of services critical for infrastructure and the security of their IT systems. (Sw. *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster*).
- The Swedish Act on Payment Services regulate payment services provided in Sweden (Sw. *Lag om betaltjänster*).
- The Swedish Trade Secrets Act prohibit disclosure of trade secrets (Sw. *Lag om företagshemligheter*).
- The Swedish Protective Security Act regulate security-sensitive organisations and their business in Sweden (Sw. *Säkerhetsskyddslag*).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The requirements under the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services are not in excess of the requirements of the NIS directive.

The abovementioned act applies to legal entities who provide services critical for infrastructure (e.g. banks and health services). The purpose of the legislation is to harmonise and improve the security of the providers of essential services and their IT systems throughout the EU.

The Swedish Protective Security Act was implemented on 1st April 2019 and places the obligation on organisations conducting activities of importance to either national security or international protective security commitments binding on Sweden. Such organisations shall work in a preventive manner to protect themselves against crimes that can threaten either the security of Sweden or the abovementioned commitments.

Also, there is currently a proposal for amendments to the Swedish Act on Electronic communications. Due to the implementation of 5G, the proposal aims to regulate radio transmitters and ensure that radio usage will not cause damage to the security of Sweden.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The GDPR puts obligations on data controllers to implement appropriate technical and organisational measures when processing personal data. Not all of these measures are explicitly defined but include to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services requires providers of services critical for infrastructure to implement appropriate and proportionate technical and organisational measures regarding their IT systems. Not all of these measures are explicitly defined but include to monitor, detect, prevent and mitigate Incidents.

Any organisation carrying out security-sensitive activities is obligated under the Swedish Protective Security Act to ascertain and document the need for security, plan and enforce necessary security measures and follow up the security work within the organisation. Also, any information of importance regarding the organisation's security shall be notified to the relevant supervisory authority. Examples of security measures can include the classification of data in certain levels of security, drafting and entering into security agreements and security screening of employees.

The Swedish Act on Electronic Communication put obligations on electronic service providers to implement appropriate technical and organisational measures regarding the services they provide. Not all of these measures are explicitly defined but include to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Payment Services ensures that providers of payment services must implement technical and organisational measures to ensure safe money transactions. As with previously mentioned laws, no explicit definitions of the measures are present but include to monitor, detect, prevent and mitigate Incidents.

Governmental Authorities shall follow the regulations drafted by the Swedish Civil Contingencies Agency. The regulations include, for example, drafting security policies and documenting security actions taken.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

As of now, no issues regarding conflict of laws have been brought to attention. The GDPR and The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services may apply at the same time but regulate different aspects. Electronic service providers subject to the Swedish Act on Electronic Communication has been explicitly excluded from the scope of The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services.

Criminal offences regarding data breach is subject to The Swedish Penal Code which does not interfere with applicable data protection law.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Data controllers subject to the GDPR are obligated to notify the Swedish Data Protection Authority without undue delay when becoming aware of a personal data Incident that is not considered to be of minor importance. The notification must include a description of the nature of the Incident (e.g. number of affected individuals and categories of data subjects). The data controller also needs to communicate its contact details, likely consequences of the personal data breach and describe measures taken/proposed to be taken to address the data breach (including appropriate measures to mitigate possible adverse effects).

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services requires providers of services critical for infrastructure (e.g. banks and health services) to report Incidents to the Swedish Civil Contingencies Agency without undue delay. Provisions explicitly defining what information an Incident report shall include are to be set out in the regulations of the supervisory authority.

The Swedish Protective Security Act obligates organisations conducting security-sensitive activities to notify the relevant supervisory authority (which may be either the Swedish Security Service or the Swedish Armed Forces depending on the situation) if, e.g., an Incident occurs in an information system.

The Swedish Act on Electronic Communication puts obligations on electronic service providers to notify severe interruptions to The

Swedish Post- and Telecom Authority without undue delay. The provider shall notify the Swedish Post- and Telecom Authority within 24 hours of an integrity Incident being discovered. An Incident is defined as an unlawful destruction, loss or change of, or unlawful disclosure or access to, information. The provider must also notify affected subscribers with information (for example, when the Incident occurred, recommended measures, contact details).

The Swedish Act on Payment Services obligates providers of payments services to report Incidents in their operations to the Swedish Financial Supervisory Authority. The notifications shall be sent without undue delay. The providers shall also notify affected individuals. The notification must include information about the Incident and how to mitigate the damage.

As a general rule, the Principle of Public Access to Official Records (Sw. *Offentlighetsprincipen*) gives individuals the right to request and access documents received by a governmental agency. Upon such request, the Swedish Data Protection Authority carries out a test, to ascertain whether the Incident report is subject to confidentiality or not. To date, The Swedish Data Protection Authority has not granted any requests regarding making an Incident report public.

To summarise, precisely what information is to be provided in relation to an Incident is not always stated in law and will depend on the Incident in question.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations are permitted to voluntarily share information with regulatory and/or other authorities and organisations, subject to compliance with any secrecy restriction which may apply under law. If the information includes personal data, the GDPR applies.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

According to the GDPR, data controllers shall communicate the personal data breach to the data subject without undue delay if the personal data breach is likely to result in a high risk to the rights and freedoms of the affected natural persons.

Subscribers to electronic services affected by an Incident have the right to be informed by the service provider without undue delay according to the Swedish Act on Electronic Communications.

The Swedish Act on Payment Services puts obligations on providers of payment services to report Incidents to the users of the payment services if there is a risk that their transactions may be affected.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Any information relating to an identified or identifiable person constitutes personal data which needs to be processed in accordance with the GDPR. Therefore, a data controller is not permitted to communicate information regarding a data breach without, e.g., legal grounds and purpose, e.g., a data controller could probably argue that processing personal data regarding a cyber threat actor in order to report such actor to the police would be in the legitimate interest of the data controller.

Also, price-sensitive information may be subject to the Swedish Trade Secrets Act, which under certain circumstances prohibits, e.g., the disclosure of trade secrets to the public.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The GDPR authorises the Swedish Data Protection Authority to monitor and enforce the application of the GDPR. This includes many different tasks such as conducting investigations, promote public awareness, handle complaints and give advice.

The NIS directive implemented in Swedish law stipulates that the Swedish Civil Contingencies Agency shall carry out supervision to ensure that providers of services critical for infrastructure (e.g. banks and health services) abide by the security measures that the law prescribes.

The Swedish Protective Ordinance supplementing the Act designates different regulators depending on the activities conducted by the organisation in question. For example, the Swedish Defence Department is subject to supervision by the Swedish Armed Forces, and individual operators who conduct operations related to electronic communications and postal service are subject to supervision by The Swedish Post- and Telecom Authority. The Swedish Security Service exercises supervision of some of the Swedish authorities as well as the municipalities and county councils of Sweden.

The Swedish Act on Electronic Communication states that The Swedish Post- and Telecom Authority is responsible for monitoring the electronic service providers compliance with the law.

The Swedish Act on Payment Services authorises the Swedish Financial Supervisory Authority to carry out supervision regarding providers of payments services.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The GDPR prescribes that a failure to report an Incident involving personal data and/or to implement appropriate technical and organisational measures can result in a fine. The fine varies depending on the infringement and can under certain circumstances amount to either 10,000,000 EUR or 2% of the data controller's total worldwide annual turnover of the preceding financial year, whichever is higher.

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services prescribes that failure to comply with the law will result in a fine starting at a minimum of 5,000 SEK with a maximum of 10,000,000 SEK.

Not complying with The Swedish Act on Electronic Communication can result in a fine or a maximum of six months in jail. Legal entities violating the law shall pay damages to the injured party.

A violation of The Swedish Act on Payment Services can result in a fine starting at a minimum of 5,000 SEK with a maximum of 50,000,000 SEK.

The penalty for violating the Swedish Trade Secrets Act is to pay damages.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The Swedish Data Protection Authority initiated its first investigations in June 2018 to verify compliance with the GDPR among companies in Sweden. In most cases where non-compliance was found, penalties such as warnings and injunctions were enforced. The first administrative sanction in Sweden was imposed in August 2019 on a public school. The public school had used facial recognition to check school attendance, which was found to be in violation of the GDPR and therefore the school was fined 200,000 SEK by the supervisory authority.

However, companies have been subject to measures before the entry into force of the GDPR. The Swedish Data Protection Authority forced a large debt collection company to introduce more mechanisms to ensure a higher level of safety for the personal data processed by the company. The company appealed against the decision but lost.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

The use of web beacons is permitted subject to The Swedish Act on Electronic Communication and the GDPR.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

The use of honeypots is not explicitly regulated in Swedish law, but measures that would be considered a so-called sting operation, i.e. enticing someone to commit a crime, is prohibited.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

Neither is the use of sinkholes explicitly regulated in Swedish law, but any re-directing must be consented to by the operator of the sinkhole. Furthermore, operating a sinkhole can result in legal difficulties depending on what kind of information will be received.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Companies and organisations can implement standards such as ISO 27002:2013 and NIST 800-88 to ease the process of regulatory compliance. These standards are not mandatory, and it is hard to draw any general conclusion about which business sectors who are more likely to implement or not. The financial and telecom sectors are more regulated than other business areas.

The Swedish Standards Institute (SSI) is a part of the European Committee for Standardisation. SSI provides standards to its members and always adopts the European standard. Currently 1,300 companies, agencies and organisations are members.

In regulated areas such as the energy area, the standards follow on from law and regulation.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

The Swedish Financial Supervisory Authority drafts regulations and guidelines regarding the financial sector. According to the regulations, the affected companies shall have a structure and management for IT security involving, for example, physical security measures, reporting systems and control of access to information.

The GDPR put obligations on data controllers to implement appropriate technical and organisational measures when processing personal data. Not all of these measures are explicitly defined but include to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services requires providers of services critical for infrastructure to implement appropriate and proportionate technical and organisational measures regarding the systems they use. Not all of these measures are explicitly defined but include to monitor, detect, prevent and mitigate Incidents.

The Swedish Act on Electronic Communication put obligations on service providers to implement appropriate technical and organisational measures regarding the services they provide. Not all of these measures are explicitly defined but include to monitor, detect, prevent and mitigate Incidents.

If an organisation in the financial services sector or telecommunications sector provides services deemed security-sensitive, the Swedish Protective Act will apply and the organisation will have to ascertain and document the need for security, plan and enforce necessary security measures and follow up the security work within the organisation. Also, any information of importance regarding the organisation's security shall be notified to the relevant supervisory authority.

The Swedish Act on Payment Services ensures that providers of payment services must implement technical and organisational measures to ensure the safety of money transactions. As with previous mentioned laws, no explicit definitions of the measures are present but include to monitor, detect, prevent and mitigate Incidents.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are no such obligations for directors. Anyone who is in breach of the laws mentioned in question 3.2 can be held responsible and charged with a fine. Violations of the Swedish Act on Electronic Communication can result in imprisonment if the breach is carried out by an individual.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The GDPR, The Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services, The Swedish Protective Act and the Swedish Act on Electronic Communications all require but do not define technical and organisational measures.

The technical measures required would likely be assessed based on market standard and best practice and might include that service providers of critical infrastructure have to carry out penetration tests in order to be compliant with the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services. It is also possible that organisational measures include that a data controller needs to establish a written Incident response plan in order to be compliant with the GDPR.

However, no applicable law is explicitly putting obligations on private or listed companies to, e.g., designate a CISO.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Listed companies are required to disclose any information (regardless of whether it derives from a cybersecurity breach or not) that may affect the price of the company shares according to the Swedish Act on Market Abuse.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are no explicit obligations under law placed upon private or listed companies regarding cybersecurity in Sweden.

Listed companies are subject to soft law (Sw. *Svensk kod för bolagsstyrning*) which states that the board of directors in a listed company should have the competence to manage the company with integrity and efficacy. Therefore, one can expect a listed company to implement satisfactory measures for ensuring a reasonable level of IT security.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

A person or a company can seek monetary remedies in court for data breaches occurring from a contractual relationship. Such breaches and the consequences thereof are often regulated in the agreement between the parties.

Data subjects may file a lawsuit against a data controller for processing personal data without legal grounds, transferring personal data to a third party without prior permission, or not assisting the data subject to exercise its data subject rights according to the GDPR. Such violations can result in damages to the data subject.

The data subjects are also able to claim for a declaratory judgment regarding its own rights (e.g. the right to be forgotten).

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Private litigation regarding cybersecurity is uncommon in Sweden. In 2013, a plaintiff was recognised damages of 3,000 SEK by the Supreme Court in a civil case regarding the publishing of a judgment on a public website. The publishing was found to violate the plaintiff's personal integrity according to the current data protection legislation.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The Swedish Tort Liability Act (Sw. *Skadeståndslagen*) is subsidiary to other laws and hence where the GDPR regulates the data subjects' right to monetary damages, this will apply instead. The act is also dispositive in a contractual context, i.e. parties to a contract are free to regulate the consequences of an Incident differently between themselves.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

It is possible to take out insurance against claims from third parties due to data breach. Fines imposed by regulatory authorities might be possible to insure against, but the legal situation is not clear. The nature of the fine (e.g. punitive or not) and the conduct (e.g. mere negligence, gross negligence or intent) are factors that need to be considered.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No. However, it is unclear whether it is possible to insure yourself against regulatory fines or not.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

An employer has the possibility to monitor employees to the extent this is necessary and justified considering the circumstances at hand. An employer may, e.g., monitor an employee's computer in order to verify that agreed security routines are upheld, provided that the employee has been informed in advance that such monitoring may be performed. Private files may not be accessed except for in cases of serious suspicion of disloyal or criminal behaviour. Hence, an employer should exercise caution and be restrictive when it considers monitoring its employees. Furthermore, if the monitoring of the

employees constitutes processing of personal data, the GDPR applies. The relation between an employee and an employer is considered to have an inherent imbalance of power, with the employee not being in a completely independent position, and therefore an employee is normally considered not to be able to freely consent to monitoring. Instead the employer will need to ensure that such supervision is based on an alternative legal ground.

Due to the duty of loyalty arising from the employment contract, an employee may have to report Incidents to the employer.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The Swedish Act on Whistleblowing offers protection to employees disclosing information on severe misconduct in the workplace or in the employer's business. Severe misconduct is aimed at acts that would be punishable by imprisonment or equivalent offences. If the information is obtained through a criminal offence according to the Swedish Penal Code (e.g. hacking), the employee is not protected against reprisals.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

If the Incident is a criminal offence according to the Swedish Penal Code (or constitutes imprisonment), the Swedish Police and the Swedish Security Service have the authorisation to investigate. The latter is more usual regarding terrorism offences.

Incidents regarding personal data are subject to the Swedish Data Protection Authority. If the Incident is affecting the IT systems of providers of critical infrastructure, the Swedish Civil Contingencies Agency is the investigating power.

The Swedish Protective Ordinance supplementing the Act designates different regulators depending on the activities conducted by the organisation in the scope of the act. For example, the Swedish Defence Department is subject to supervision by the Swedish Armed Forces, and individual operators that conduct operations related to electronic communications and postal service are subject to supervision by The Swedish Post- and Telecom Authority. The Swedish Security Service exercises supervision of some of the Swedish authorities as well as the municipalities and county councils of Sweden.

The Swedish Post- and Telecom Authority is responsible for investigating service providers who fail to report Incidents.

The Swedish Financial Supervisory Authority is authorised to investigate crimes regarding the Swedish Act on Payment Services.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Providers of electronic communication services are obligated upon request from law enforcement authorities to provide personal data if there is a suspicion of serious crime. The ECJ ruled in the Joined Cases C-203/15 and C-698/15 that such a request for disclosure shall be subject to preliminary review by a court or an independent administrative authority.

Anders Hellström has more than 12 years of experience as a commercial lawyer, starting out at Bird & Bird in 2006 and moving to Synch when it was founded in 2014. Prior to that, he served as an assistant judge at the District Court of Östersund between 2003–2005. During his career he has also been seconded to two major IT service providers for a total time of almost one year. Anders' focus area is commercial law, mainly working with companies in the IT and technology services sectors. He regularly provides advice to clients in commercial cases, assisting in a wide range of different matters and contracts, including licence agreements, outsourcing deals, service agreements and negotiations.

Synch Advokat
AB, P.O. Box 3631
SE-103 59 Stockholm
Sweden

Tel: +46 761 761 990
Email: anders.hellstrom@synchlaw.se
URL: www.synchlaw.se

Erik Myrberg joined Synch in 2018 and works as a junior lawyer contributing to the commercial and data privacy practice of the firm. Erik acquired his Master of Laws degree from Uppsala University in 2018, focusing his Master's studies in the GDPR. He also studied courses in IT law, business law and EU law at Wirtschaftsuniversität Wien.

Synch Advokat
AB, P.O. Box 3631
SE-103 59 Stockholm
Sweden

Tel: +46 761 761 948
Email: erik.myrberg@synchlaw.se
URL: www.synchlaw.se

Founded in 2014, Synch is a Nordic law firm focused on innovation, digital business and technology. Our business objective is to simplify the management of legal matters. In doing so we disrupt the Nordic market for legal services by introducing innovative digital technology in our operations as well as offering digital services to our clients.
The Synch legal offering includes Advisory Services, Project & Transactional Services, Managed Services and Digital Services. Our focus lies within the market verticals Venture Capital, Industrial & Resources, Health & Life Sciences, Digital Business and Retail. We work with start-up high-growth businesses, established industrial companies looking to improve their business processes and mature corporations seeking new opportunities to diversify their business offering.

In five years, Synch has evolved to a legal firm with over 60 employees with representation in Sweden, Denmark, Norway and the Silicon Valley. Our turnover has in average grown by 30–50% annually.

www.synchlaw.se

Switzerland

Clara-Ann Gordon

Dr. András Gurovits

Niederer Kraft Frey Ltd.

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking can constitute a criminal offence in Switzerland. Pursuant to Article 143*bis* of the Swiss Criminal Code (SCC), any person who obtains unauthorised access by means of data transmission equipment, to a data processing system that has been specially secured to prevent such access, is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. If the hacker for their own or for another's unlawful gain obtains specially secured data which is not intended for them, they are liable, according to Article 143 SCC, to a custodial sentence not exceeding five years or to a monetary penalty.

In its decisions BGer 6B_615/2014 and 6B_456/2007, the Swiss Federal Supreme Court held that unauthorised access to another person's password-protected email account falls under the scope of the "hacking offence". In 2016, several hackers and persons threatening to hack IT systems of banks, universities and private enterprises could have been identified and arrested in Switzerland or abroad with the help of mutual legal assistance from foreign authorities.

Denial-of-service attacks

Denial-of-service attacks can constitute a criminal offence in Switzerland. Pursuant to Article 144*bis* SCC, any person who without authorisation alters, deletes or renders unusable data that is stored or transmitted electronically is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. Moreover, data can also be regarded as rendered unusable if such data still exists but is temporarily inaccessible for authorised users, e.g. due to a denial-of-service attack.

Moreover, depending on the *modus operandi* of the individual case, the following further criminal provisions can be applicable in the context of denial-of-service attacks:

- extortion (Article 156 SCC) – penalty: a custodial sentence not exceeding five years; or a monetary penalty;
- coercion (Article 181 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- misuse of a telecommunications installation (Article 179*septies* SCC) – penalty: a fine upon complaint; and
- obstructing, disrupting or endangering the operation of a telecommunication service or utility provider (Article 239 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty.

Phishing

Depending on the individual design and purpose of a phishing mail or website, such phishing can constitute the following criminal offences:

- fraudulent use of a trademark or a copyright-protected work (Article 62 of the Swiss Trade Mark Protection Act, Article 67 of the Swiss Copyright Act);
- forgery of a document (Article 251 SCC); or
- computer fraud: unauthorised use of data and the transferring of financial assets through phishing (Article 147 SCC),

each of which is punishable by a custodial sentence not exceeding five years, or by a monetary penalty if committed for commercial gain.

Furthermore, in phishing cases, the criminal offence of money laundering (Article 305*bis* SCC), with a penalty of a custodial sentence not exceeding three years or a monetary penalty, can be part of the accusation (see the decision by the Swiss Federal Criminal Court, BG.2011.43).

The Office of the Attorney General of Switzerland has reported that, from 2012 to 2016, 455 criminal complaints with regard to phishing were filed by banks, authorities and private persons. Many cases were closed without an outcome due to lack of evidence or offenders remaining unidentified. Other cases, especially those involving requests for mutual legal assistance of foreign authorities, are still pending. As per the end of 2018, 173 cases of phishing are still pending.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Such infections can be covered by Article 144*bis* SCC, prescribing that whoever alters, deletes or renders unusable data that is stored or transmitted electronically is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty ("virus offence").

Especially in connection with ransomware attacks, the following further criminal provisions can be applicable:

- fraud for commercial gain (Article 146 SCC) – penalty: a custodial sentence not exceeding 10 years; or a monetary penalty of not less than 90 daily penalty units;
- extortion (Article 156 SCC) – penalty: a custodial sentence not exceeding five years; or a monetary penalty; and
- money laundering (Article 305*bis* SCC) – penalty: a custodial sentence not exceeding three years; or a monetary penalty.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

While the mere possession of hacking tools is not illegal, the provision or use of hacking tools can constitute a criminal offence. According to Article 144*bis* paragraph 2 SCC, whoever manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that will be used to alter, delete or render unusable data without authorisation is liable to a custodial sentence

of up to three years or to a monetary penalty. In its decision BGE 129 IV 230, the Swiss Federal Supreme Court held that instructions and manuals explaining how to create programs that infect, destroy or render data unusable fall under the scope of this virus offence.

Moreover, any person who markets or makes accessible passwords, programs or other data that are intended to be used to obtain unauthorised access to a data processing system is liable to a custodial sentence not exceeding three years or to a monetary penalty as prescribed by Article 143*bis* paragraph 2 SCC.

Finally, exporting or brokering certain goods for monitoring the internet or mobile telecommunications without official permission can be liable to a custodial sentence of up to three years or to a monetary penalty pursuant to Article 9 of the Ordinance on the Export and Brokering of Goods for Monitoring Internet and Mobile Communication.

Identity theft or identity fraud (e.g. in connection with access devices)

There is no explicit regulation for identity theft or identity fraud in Switzerland. Depending on the intention of the offender and his *modus operandi*, it can be covered by different articles of the SCC, such as Article 143 (unauthorised obtaining of data), Article 146 (fraud), Article 147 (computer fraud), Article 143*bis* (hacking) or Article 173 *et seqq.* (offences against personal honour).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft can be covered by several criminal offences. Article 143 SCC prescribes the penalty for an unauthorised data acquisition. The maximum penalty is a custodial sentence of five years. Furthermore, any person who betrays a manufacturing or trade secret that is not to be revealed under a statutory or contractual duty, or anyone who exploits such a betrayal, can face a custodial sentence of up to three years or a monetary penalty under Article 162 SCC. Finally, according to Article 67 *et seqq.* of the Swiss Copyright Act, a copyright infringement that has been committed wilfully and unlawfully can be punished with a custodial sentence of up to one year or a monetary penalty; in cases of committing the offence for commercial gain, the penalty is a custodial sentence not exceeding five years or a monetary penalty.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The following further criminal offences impairing security, confidentiality, integrity and availability have to be considered under Swiss law:

- falsification or suppression of information in connection with a telecommunications service (Article 49 of the Swiss Telecommunications Act (TCA)) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- unauthorised misuse or disclosure of information received by means of a telecommunications installation that was not intended for the receiver (Article 50 TCA) – penalty: a custodial sentence of up to one year; or a monetary penalty;
- interfering in telecommunications or broadcasting (Article 51 TCA) – penalty: a custodial sentence of up to one year; or a monetary penalty;
- obstructing, disrupting or endangering the operation of a telecommunication service or utility provider (Article 239 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- breach of professional confidentiality (Article 321 SCC) – penalty: a custodial sentence of up to two years; or a monetary penalty. Article 35 of the Swiss Federal Act on Data Protection (FADP) – penalty: monetary penalty. Article 47 of the Banking Act – penalty: a custodial sentence of up to three years; or a monetary penalty. Article 147 of the Financial Market Infrastructure Act (FMIA) – penalty: a custodial sentence not exceeding three years; or a monetary penalty;
- breach of postal or telecommunications secrecy (Article 321ter SCC) – penalty: a custodial sentence not exceeding three years; or a monetary penalty. Articles 43 and 53 TCA – penalty: fine not exceeding CHF 5,000; and
- unsolicited distribution of spam massages (Article 3 *lit. o* in conjunction with Article 23 of the Swiss Federal Law on Unfair Competition) – penalty: a custodial sentence of up to three years; or a monetary penalty.

Failure by an organisation to implement cybersecurity measures

There is no generally applicable regulation in Switzerland specifically requiring the implementation of certain cybersecurity measures (for sector-specific requirements, see question 3.2 below). However, general compliance obligations require the implementation of an internal control system (relevant for companies limited by shares, see Article 20 of the Swiss Code of Best Practice for Corporate Governance) and technical and organisational measures to ensure the confidentiality, integrity and availability of information and IT systems, which can include the implementation of an adequate information security management system (relevant for all organisations, see Article 7 FADP).

The Swiss Federal Council adopted the second "National Strategy on Switzerland's Protection against Cyber Risks" (NCS) in 2018 for the years 2018–2022. The strategy builds on the work of the first NCS (2012–2017), expands it where necessary and supplements it with new measures so that it corresponds to the current threat situation. It was developed in collaboration with industry, the cantons and universities and thus forms the basis for the necessary joint efforts to reduce cyber risks.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The extraterritorial application of the SCC, with regard to the offences mentioned above, requires that the offender is present in Switzerland and will not be extradited (Articles 6, 7 SCC). In the context of phishing, it is currently in dispute between the Swiss Office of the Attorney General and the criminal courts whether, on the basis of the Council of Europe's Cybercrime Convention in conjunction with Article 6 SCC, such offences committed abroad are even subject to Swiss criminal jurisdiction where the offender and victim are not Swiss citizens.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, Swiss criminal law incorporates the mitigating principles of withdrawal and active repentance. If a person of his own accord does not complete the criminal act. or if he assists in preventing the completion of the act, the court may reduce the sentence or waive any penalty (Article 23 SCC).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The following other provisions can be applicable in the context of cybersecurity:

- causing fear and alarm among the general public (Article 258 SCC);

- public incitement to commit a felony or act of violence (Article 259 SCC);
- participating in or supporting a criminal organisation (Article 260*ter* SCC);
- financing terrorism by collecting or providing funds (Article 260*quinquies* SCC);
- foreign operations and activities directed against the security of Switzerland (Article 266*bis* SCC);
- diplomatic treason: endangering the interest of Switzerland: (i) by making a secret accessible to a foreign country; or (ii) by falsifying, destroying, disposing of or stealing documents relating to Switzerland's legal relations with a foreign state (Article 267 SCC);
- political, industrial or military espionage in the interest of a foreign state or organisation (Articles 272, 273, 274 SCC);
- founding of an unlawful association (Article 275*ter* SCC); and
- criminal provisions concerning the representation of acts of violence (Article 135 SCC), pornography (Article 197 SCC) or racial discrimination (Article 261*bis* SCC).

Please note the decisions of the Swiss Federal Criminal Court, SK.2013.39, and the Swiss Federal Supreme Court, BGer 6B_645/2007, both regarding cases of "cyber-jihad/cyber-terrorism", included several of the above-mentioned offences as part of the subject of the accusation.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The Applicable Laws are as follows:

- Federal Act on Data Protection.
- Ordinance to the Federal Act on Data Protection.
- Swiss Criminal Code.
- Telecommunications Act.
- Ordinance on Telecommunications Services.
- Federal Act on Copyright and Related Rights.
- Trade Mark Protection Act.
- Civil Code, Code of Obligations.
- Banking Act.
- Ordinance on Banks.
- Financial Market Infrastructure Act.
- Financial Market Supervision Act.
- Federal Law on Unfair Competition.
- Federal Act on the Implementation of International Sanctions.
- Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods.
- Ordinance on the Export, Import and Transit of Dual Use Goods, Specific Military Goods and Strategic Goods.
- Ordinance on the Export and Brokering of Goods for Monitoring Internet and Mobile Communication.
- Federal Act on the Intelligence Service.
- Federal Information Security Act.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

In Switzerland, there are no generally applicable mandatory cybersecurity requirements for critical infrastructures so far (for sector-specific requirements, see question 3.2 below). In 2017, the Swiss Federal Council adopted the "National Strategy on the Protection of Critical Infrastructures" (SKI) for the years 2018–2022. The Swiss Federal Office for Civil Protection was mandated to implement the strategy and published a "Guideline for the Protection of Critical Infrastructures" in 2015 (updated in 2018), outlining recommended risk, crisis and continuity concepts based on international standards. Furthermore, the Swiss Federal Information Security Act prescribes certain security measures for Swiss Federal authorities and offers support to private operators of critical infrastructures to minimise network and system disruptions.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There is no generally applicable requirement in Switzerland to take measures to monitor, detect, prevent or mitigate Incidents. However, Article 7 FADP in conjunction with Articles 8 and 9 of the Ordinance to the FADP provide that personal data must be protected against unauthorised processing, destruction, loss, technical faults, forgery, theft or unlawful use through the implementation of adequate technical and organisational measures including mandatory controls of the following IT and data-related circumstances: entrance; personal data carrier; transport; disclosure; storage; usage; access; and input.

With regard to specific cybersecurity safeguards to be implemented in the financial and telecommunications sector, see question 3.2 below.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Such conflicts of laws cannot currently be perceived.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

So far, there is no general reporting obligation for cyberattacks in Switzerland. However, a duty to notify the Swiss Federal Data Protection and Information Commissioner in cases of unauthorised data processing or loss of data has been included in the preliminary draft of the revised FADP. Specific reporting obligations are currently only imposed on certain industries such as the financial and the telecommunication sector, see question 3.2 below.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Organisations have the possibility (not the obligation) to inform MELANI, the Swiss Reporting and Analysis Centre for Information Assurance. Such a notification can be filed anonymously with a simple message on MELANI's website. Furthermore, it is also possible to inform the Swiss Coordination Unit for Cybercrime Control (CYCO).

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There is no such explicit obligation to inform affected individuals under Swiss law. However, in the legal literature, it is partially held that organisations are obligated to report such Incidents to the affected individuals in accordance with Article 4 paragraph 2 FADP, incorporating the principle of good faith. The necessity and extent of such information depends on the circumstances, e.g. the gravity of the breach and the necessity to prevent any damages and potential abuse of the disclosed data. The preliminary draft of the revised FADP provides for obligations to notify affected data subjects in cases of unauthorised data processing or loss of data.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The supervisory authorities monitoring and enforcing the above-mentioned requirements pertaining to general data protection and sector-specific cybersecurity are the following:

- Federal Data Protection and Information Commissioner.
- Cantonal Data Protection Commissioners.
- Federal Office of Communications (OFCOM).
- Financial Market Supervisory Authority (FINMA).

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Due to the absence of a general obligation to implement safeguards against cyberattacks or to report Incidents to an authority, there are no penalties for not complying.

For penalties triggered by not complying with sector-specific obligations to report Incidents to the supervisory authorities, see question 3.2 below.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

So far, to our knowledge, the competent supervisory authorities have enforced sector-specific reporting provisions only in cases that had no connection with cybersecurity. However, in 2016, FINMA ordered banks of supervisory category 1 (extremely large, important and complex market participants; very high risk) and category 2 (very important, complex market participants; high risk) to conduct an additional examination and invited those of category 3 (large and complex market participants; significant risk) to conduct a self-assessment pertaining to the status of the implementation of safeguards against cyberattacks.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no general permission or prohibition for organisations to use Beacons; however, each organisation must analyse whether with the use of this measure, and the way it is used, provisions of the Swiss Criminal Act, Data Protection Act, Unfair Competition Act, etc. could be infringed. The Swiss Federal Intelligence Service (FIS) is subject to certain conditions permitted to use such kind of measures based on the Federal Act on the Intelligence Service.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There is no general permission or prohibition for organisations to use Honeypots, however each organisation must analyse whether with the use of this measure and the way it is used, provisions of the Swiss Criminal Act, Data Protection Act, Unfair Competition Act, etc. could be infringed. The Swiss Federal Intelligence Service (FIS) is permitted to use such kind of measures, subject to certain conditions, based on the Federal Act on the Intelligence Service.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There is no general permission or prohibition for organisations to use Sinkholes; however, each organisation must analyse whether with the use of this measure and the way it is used, provisions of the Swiss Criminal Act, Data Protection Act, Unfair Competition Act, etc. could be infringed. The Swiss Federal Intelligence Service (FIS) is permitted to use such kind of measures, subject to certain conditions, based on the Federal Act on the Intelligence Service.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, market practice varies across business sectors as the legal requirements are different (see question 3.2 below).

In addition, please note that, on 18 April 2018, the Swiss Federal Council adopted "The National Strategy for the Protection of Switzerland against Cyber Risks" which will certainly impact all sectors in Switzerland.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) Yes, Article 14 of the Financial Market Infrastructure Act (FMIA) requires financial market infrastructures (*i.a.* stock exchanges, trading facilities, payment systems) to operate robust IT systems which are appropriate for their activities, provide for effective emergency arrangements, ensure the continuity of business activity, and provide for measures to protect the integrity and confidentiality of information regarding their participants and their transactions. Article 3f of the Banking Act and Article 12 paragraph 4 of the Ordinance on Banks require banks to implement appropriate risk management, including an internal control system, in order to detect, limit and monitor, *i.a.*, relevant operational risks. These requirements are specified in the recently updated FINMA Circular 2008/21 "Operational Risks – Banks" where the minimum details of a cyber risk management concept to be implemented based on international standards are outlined (protection of processes/IT systems/sensitive data, detection and recording of cyberattacks, remedial measures, recovery of normal operations, regular vulnerability analysis and penetration testing). FINMA Circulars are not legally binding, but they elaborate the regulator's intended enforcement practice and are regularly accepted and complied with by the industry.

According to Article 29 paragraph 2 of the Financial Market Supervision Act (FINMASA), FINMA has to be informed about any Incident that is of substantial importance to supervision, which can include Incidents that could have a negative impact on the reputation or operation of the financial institution or the financial centre of Switzerland. Pursuant to Articles 45 and 46 FINMASA, the wilful provision of false information to FINMA or failing to make a mandatory report to FINMA can be punished with a custodial sentence of up to three years or a monetary penalty and, in cases of negligence, with a fine of up to CHF 250,000. In case of a serious infringement of the supervisory provisions, the licence of a supervised person or entity can, according to Article 37 FINMASA, be revoked, its recognition withdrawn or its registration cancelled.

(b) On the basis of Article 96 paragraph 2 of the Ordinance on Telecommunications Services (OTS), OFCOM has published a currently non-binding "Guideline on Security and Availability of Telecommunications Infrastructures and Services" recommending telecommunications service providers to implement, monitor and update: (i) an information security management system as described in the international standards relating to information security, such as ISO/IEC 27001:2005 and ITU-T X.1051; (ii) a business continuity plan; and (iii) a disaster recovery plan, and to comply with international security recommendations in the ICT sector, such as the "ETSI White Paper No. 1 – Security for ICT" and the "ITU-T ICT Security Standards Roadmap". OFCOM has the competence to declare the mentioned guideline to be binding. Article 96 OTS prescribes the obligation of telecommunications service providers to immediately inform OFCOM of disruptions in the operation of their networks which (potentially) affect at least 30,000 customers (landline, over-the-top, broadcasting) or 25 transmitter sites (mobile communications). OFCOM requires the operators to include in the report, *i.a.*, a description of the disruption, the categories of causes (cable rupture, energy/hardware/software/human failure, cyberattack, malicious interference), and the measures taken to end the disruption. Pursuant to Article 53 of the Telecommunications Act, anyone who infringes any provision of the telecommunications legislation, such as the reporting obligation under Article 96 OTS, is liable to a fine not exceeding CHF 5,000.

Finally, there are further sector-specific requirements, particularly in connection with aviation, the railway industry and nuclear energy.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

If the failure results from not having an adequate compliance management system (including risk management, internal reporting and control, and sufficient supervision) in a company limited by shares or a limited liability company, this can constitute a breach of the directors' obligation to perform their duties with all due diligence and to safeguard the interests of the company in good faith (Articles 717, 812 Code of Obligations) and to supervise the persons entrusted with managing the company, in particular with regard to compliance with the law (Article 716a Code of Obligations). These duties are only explicitly imposed on members of the board of directors, managing directors and executive officers of companies limited by shares, and managing directors of limited liability companies.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no such general obligation to designate a CISO under Swiss law.

(b) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to establish a written Incident response plan or policy.

(c) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to conduct periodic cyber risk assessments, including for third-party vendors.

(d) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to perform penetration tests or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no generally applicable disclosure requirements in relation to cybersecurity risks or Incidents for companies in Switzerland (for sector-specific requirements, see question 3.2 above). However, if an Incident may result in damage claims or penalties, these risks have to be assessed and appropriate provisions have to be established and included in the balance sheet in the annual reports.

Furthermore, in the event that a large number of data subjects are affected, there may be an exceptional duty to report the Incident publicly according to the data procession principle of good faith (see question 2.7 above). This can particularly be the case if the data subjects concerned cannot be informed individually.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

There are no other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

According to Article 15 paragraph 1 FADP in conjunction with Article 28 *et seqq.* of the Swiss Civil Code, the affected person of a cybercrime-induced data breach has the possibility to bring actions relating to the protection of privacy, provided that there is a violation of personality rights, e.g. due to data theft or illegal data processing. This can include actions for damages, prohibitive injunctions, information/disclosure and notification of third parties or the publication of judgments. Furthermore, members of the board of directors, managing directors and executive officers of companies limited by shares, and managing directors of limited liability companies, are liable both to the company and to the individual shareholders and creditors, for any losses or damage arising from any intentional or negligent breach of their duties (Articles 754, 827 Code of Obligations); see question 4.1 above.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

To date, we are not aware of any civil actions that have been filed by affected persons or companies in relation to cybersecurity Incidents in Switzerland. The few judgments pertaining to liability for data breaches derive from administrative investigations conducted by the supervisory authorities.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

If the claimant is able to prove damages and the violation of a legally protected right or norm, the purpose of which is to protect from such damages, he is entitled to compensation for moral sufferings and the payment of damages by virtue of Articles 49 and 41 of the Code of Obligations. Furthermore, according to Article 423 of the Code of Obligations, data subjects can request the handing-over of profits arising from violations of their privacy rights.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Since 2000, organisations have the possibility to take out insurance against cyberattacks. The offered coverage includes, for example, loss or theft of data, damages due to hacking and malware, and the unauthorised disclosure of data.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations to insurance coverage concerning such Incidents.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) There are no such specific requirements.
(b) A general reporting obligation of cyber risks and other potential Incidents for employees *vis-à-vis* the employer can, according to Article 321a of the Code of Obligations, be derived from the duty of care and loyalty.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Laws with possibly inhibiting effects on reporting cyber risks and similar Incidents may be triggered by the secrecy provisions mentioned under the last heading of question 1.1 above. Furthermore, in Switzerland, there is no explicit protection for whistleblowers, so far, who report Incidents with regard to their employers to public authorities or the media. However, a draft bill of the Code of Obligations, which is still under the scrutiny of the legislative institutions, introduces such whistleblower protection from termination and other detriments (Article 336 paragraph 2 *lit.* d, Article 328 paragraph 3 Code of Obligations).

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

KOBIK, the Swiss Coordination Unit for Cybercrime, does not only function as a notification office for cybercrimes, but also looks actively for criminally relevant content on the internet. However, after its verification, KOBIK passes the information to the competent criminal law enforcement authorities, which are the local, cantonal and Swiss Federal police departments and public prosecutors' offices.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements under Swiss law.

Clara-Ann Gordon is specialised in the areas of TMT/outsourcing, data privacy, internal investigations/e-discovery and compliance. She regularly advises clients in the above areas on contractual, governance/compliance and other legal matters, represents clients in transactions and before the competent regulatory and investigating authorities as well as before state courts, arbitral tribunals and in mediation proceedings, and renders opinions on critical regulatory and contract law topics in the said industry-specific areas.
She has advised on and negotiated a broad range of national and international IT, software and outsourcing transactions (also in regulated markets), has represented clients in technology-related court proceedings and international arbitration, and is experienced in data protection and secrecy laws, white-collar investigations and e-discovery, telecom regulations (including lawful interception), e-commerce, and IT law.
Ms. Gordon regularly publishes in the field of technology (ICT) and frequently speaks at national and international conferences on emerging legal issues in technology law.

Niederer Kraft Frey Ltd.
Bahnhofstrasse 53
CH-8001 Zurich
Switzerland

Tel: +41 58 800 8426
Email: clara-ann.gordon@nkf.ch
URL: www.nkf.ch

András Gurovits specialises in technology (IT, telecoms, manufacturing, regulatory) transactions (including acquisitions, outsourcing, development, procurement, distribution), data protection, corporate, dispute resolution (including administrative proceedings) and sports.
He regularly advises clients on contractual, compliance, governance, disputes and other legal matters in the above areas.
He, thus, not only advises in these areas, but also represents clients before the competent regulatory and investigating authorities, state courts and arbitral tribunals.
Dr. Gurovits is distinguished as a leading lawyer by various directories such as *Chambers* and *The Legal 500*. Dr. Gurovits has been a lecturer at the University of Zurich for more than a decade. Presently, he is a listed arbitrator with the Court of Arbitration for Sport (CAS/TAS) in Lausanne and a member of the Legal Committee of the International Ice Hockey Federation.

Niederer Kraft Frey Ltd.
Bahnhofstrasse 53
CH-8001 Zurich
Switzerland

Tel: +41 58 800 8377
Email: andras.gurovits@nkf.ch
URL: www.nkf.ch

Taiwan

Lee and Li, Attorneys-at-Law

Ken-Ying Tseng

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Pursuant to Article 358 of the ROC Criminal Code, a person who breaks into someone else's computer or related equipment by entering another's account code and password without authorisation, breaking into the protection measure, or taking advantage of the system loophole of such system shall be sentenced to imprisonment for no more than three years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD300,000 may be imposed. Hacking, i.e., the unauthorised access of another's system, is likely to be deemed as constituting such an offence.

Denial-of-service attacks
Pursuant to Article 360 of the ROC Criminal Code, a person who, without authorisation, interferes with the computer or related equipment of another person and causes injury to the public or another through the use of computer programs or other electromagnetic methods shall be sentenced to imprisonment for no more than three years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of not more than NTD300,000 may be imposed. "Denial-of-service attacks" may be deemed as such unauthorised interference of another's computer system and may be subject to the above criminal sanctions.

Phishing
Pursuant to Article 359 of the ROC Criminal Code, a person who, without authorisation, obtains, deletes or alters the magnetic record of another's computer or relating equipment and causes injury to the public or others shall be sentenced to imprisonment of no more than five years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD600,000 may be imposed. "Phishing" in general refers to the activities of obtaining someone else's important information, such as account number and password, or personal information by using the internet, which may constitute the above offence if injury to the public or others is caused.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware may be deemed as interfering with another's computer system and altering the records in another's computer system without authorisation and may be deemed as the offences as set forth under Article 360 and/or Article 359 of the ROC Criminal Code and may be subject to the criminal sanctions as set forth above.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Pursuant to Article 362 of the ROC Criminal Code, a person who makes computer programs specifically for themselves or another to commit the offences specified as set forth under Articles 358 to 361 of the ROC Criminal Code and causes injury to the public or another shall be punished with imprisonment of no more than five years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD600,000 may be imposed. The mere possession or use of software that may be used to commit cybercrime may not be deemed as constituting the offence as set forth under Article 362 of the Criminal Code. Whether a person will be held criminally liable with regard to possessing such software will depend on the actual activities that the person conducts by possessing or using such software.

Identity theft or identity fraud (e.g. in connection with access devices)
Depending on how the identity information is stolen, the activity to obtain the identification information may constitute either the offence set forth under Article 358 or Article 359 of the ROC Criminal Code as set forth above. As for using another's identity for fraud purposes, it may constitute either the general criminal offence concerning "fraud" activity as set forth under Article 339 of the ROC Criminal Code or depending on the factual situation, constitute the criminal offence set forth under Article 339-3 of the ROC Criminal Code, which stipulates that a person who for the purpose of exercising unlawful control over other's property for themselves or for a third person takes the property of another by entering false data or wrongful directives into a computer or relating equipment to create the records of acquisition, loss or alteration of property ownership shall be sentenced to imprisonment for no more than seven years; in addition thereto, a fine of no more than NTD700,000 may be imposed. Tricking an auto-machine, such as an ATM, by stealing someone else's identity is another criminal offence under the ROC Criminal Code. Pursuant to Article 339-2, such activity may incur criminal sanction, such as imprisonment for no more than three years and/or a criminal fine of no more than NTD300,000. Whether the activities concerning identity theft or identity fraud would constitute any other criminal offence shall depend on the actual activity that was conducted.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Under Taiwan law, either infringing another's copyright or trade secret may incur criminal liabilities. In addition, an individual breaching the confidentiality obligations that he/she was imposed during his/her prior employment relationship with his/her former

employer may incur civil liability for breach of contract. If the confidential information constitutes the trade secret of the former employer, the individual may be subject to a criminal sanction of up to five years' imprisonment or short-term detention, and a criminal fine ranging from NTD1 million to NTD10 million may be imposed. If the purpose of the infringement of a trade secret is for the trade secret to be implemented or exercised in the PRC, Hong Kong or Macau, the individual may be subject to imprisonment of one to 10 years and a criminal fine of NTD3 million to 50 million may be imposed. As for infringing another's copyright, depending on the actual infringement being conducted, the amount of the criminal fine may be as high as NTD5 million, and the length of imprisonment may be as long as five years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Depending on the actual fact concerning such activity, such activity may be deemed as constituting one or more criminal offences as listed above. For example, in 2016, a group of Russians and Eastern Europeans hacked into the system of a Taiwan bank from London and remotely accessed and controlled certain ATMs of the Taiwan bank located in Taiwan and obtained cash from the machines. The individuals came to Taiwan to collect the cash, which was then seized by the Taiwan police, while the hackers outside of Taiwan remain untouched. The Russian and Eastern Europeans who were seized by the Taiwan law enforcement authorities were sentenced to criminal sanctions including imprisonment for having committed almost all of the above-mentioned criminal offences.

Failure by an organisation to implement cybersecurity measures
Pursuant to the Personal Data Protection Act of Taiwan (the "PDPA"), all organisations shall adopt proper security measures to protect the personal data that they retain. Under the PDPA, breaching such obligation will not incur criminal liability unless the organisation, with the intention to gain illegal benefit or damaging others' benefit for itself or a third party, breaches the obligation on purpose to illegally alter, delete or otherwise damage the accuracy of the personal data files of others, therefore causing or threatening to cause injury to others.

If an organisation is designated by its competent authority to be one of the non-public organisations providing "critical infrastructure" that shall be subject to the cybersecurity obligations under the Cybersecurity Management Act and the organisation fails to comply with the relevant requirements, the Cybersecurity Management Act does not stipulate any criminal liability.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The relevant statutes do not "spell out" any extraterritorial application but whether those will have extraterritorial application shall be subject to the general provisions under the ROC Criminal Code. If the relevant actions cause any consequence in Taiwan or one of the elements of the actions is conducted in Taiwan, the Taiwan court will have jurisdiction over such offences and the ROC Criminal Code will become applicable.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The relevant statute does not stipulate any specific reporting or notification mechanism that can exempt the offender from the relevant penalties. It seems that other than "surrendering himself/herself" to the law enforcement authority, there is no other mechanism that can reduce the criminal liability.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

There is one general offence stipulated under the National Security Act which may subject an individual to imprisonment for a term of not more than five years or short-term detention and, in addition thereto, a fine of not more than NTD1 million may be imposed if this individual is deemed to have conducted activities that "endanger national security or social stability" or is deemed to be acting as a spy for foreign countries, the PRC, Hong Kong or Macau. Theoretically, this clause may be applicable to cybersecurity matters. Meanwhile, to tackle "fake news", "mis-information" and the "information wars" arising from the up-coming election or from the other side of the strait, the ruling party of the Taiwan government is proposing to amend the National Security Act to cover such situations and activities, which may be in relation to cybersecurity.

Furthermore, if the purpose of conducting the relevant activities is to assist in "terrorism activities", the individuals conducting the relevant activities may be subject to various criminal sanctions as set forth under the Counter-Terrorism Financing Act, including imprisonment of no more than five years or a criminal fine of no more than NTD5 million. The criminal liabilities under the Money Laundering Control Act may also become applicable.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The following Taiwan statutes may be relevant to cybersecurity:
1. Cybersecurity Management Act;
2. Personal Data Protection Act;
3. Criminal Code (the relevant offences in regard to computer crime and fraud, etc.);
4. The Communication Security and Surveillance Act;
5. Trade Secret Act;
6. Copyright Act;
7. Patent Act;
8. National Security Act;
9. Counter-Terrorism Financing Act; and
10. Regulation Governing Export and Import of Strategic High-Tech Commodities.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Yes. On June 6, 2018, the very first cybersecurity legislation of Taiwan, the Cybersecurity Management Act, became an official

statute of Taiwan and took effect on January 1, 2019. The Executive Yuan has promulgated a series of rules and regulations since November 2018, including the Enforcement Rules of the Cybersecurity Management Act, "Regulations for Classification of Cybersecurity Responsibility", "Regulations for Reporting and Responding Cybersecurity Incidents", "Regulations for Inspecting Implementation Status of Specific Non-Governmental Agencies' Cybersecurity Maintenance Programs", "Cybersecurity Information Sharing Regulations" and "Award and Punishment Regulations on Cybersecurity Affairs for the Public Servants".

Pursuant to the Cybersecurity Management Act and the above regulations, such as the Regulations for Classification of Cybersecurity Responsibility, cybersecurity responsibility is further classified into five levels (from Level A to Level E). Each government agency must stipulate its own cybersecurity maintenance plan and also set forth the guidelines on the cybersecurity matters for the "specific non-governmental agencies" that it regulates. Many government agencies have promulgated such guidelines to regulate the "specific non-governmental agencies" subject to their jurisdiction. For example, the regulator of the telecommunications and broadcasting industries, the National Communication Commission (the "NCC"), promulgated the "Regulations of Specific Non-Governmental Agencies' Cybersecurity Management by the National Communications Commission" on April 1, 2019.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Cybersecurity Management Act requires Taiwan government agencies as well as the specific non-government agencies to adopt cybersecurity maintenance plans and report any cybersecurity Incident to the relevant government authorities. Each of the competent authorities has issued guidelines for adopting cybersecurity plans in this regard for the reference of the businesses that are subject to their jurisdictions. In such guidelines, general security standards, including ISO27001, were referred to and recommended. Although, in such general securities standards, there is no reference to the specific obligation that shall be imposed on a government agency or a non-government agency with regard to the monitoring, detecting, preventing or mitigating the occurrence of any Incidents, reference to implementing anti-virus measures or adopting periodical checks on the security procedures were made. In sum, the obligations that a government agency or a specific non-government agency is imposed with are a general security obligation.

With regard to personal data protection, a private organisation is required to take proper security measures to protect the personal data that it holds so that the personal data will not be stolen, altered, damaged, or lost. The competent authority of each industry has the power to require the private organisations under its jurisdiction to stipulate personal data file security maintenance plans.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

In theory, conflict-of-law issues may arise when protecting cybersecurity in Taiwan, especially if the attack came from overseas. But note again that there are no specific requirements referred to in question 2.3 stipulated under Taiwan law. There is only the general cybersecurity protection obligation.

Meanwhile, Taiwan does adopt export/import controlling measures which are similar to those adopted by the US and EU, and encryption software and hardware may be subject to the relevant export/import controlling requirements.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Pursuant to the Cybersecurity Management Act, the agencies subject to the Cybersecurity Management Act shall report to their supervisory agency or to the competent authority of the industry that the private agency is engaging in as applicable when the agency becomes aware of a cybersecurity Incident. A cybersecurity Incident refers to any Incident under which the system or information may have been accessed without authorisation and used, controlled, disclosed, damaged, altered, deleted, or otherwise infringed, affecting the function of the information communication system and thereby threatening the cybersecurity policy.

The "Regulations for Reporting and Responding to Cybersecurity Incidents" set forth further details about the reporting of a cybersecurity Incident as required under the Cybersecurity Management Act. A "specific non-government agency" shall report to its regulator at the central government within "one hour" after it becomes aware of the cybersecurity Incident and the regulator shall respond within two to eight hours depending on the classification of the cybersecurity Incident. Meanwhile, the specific non-government agency shall complete damages control or recovery of the system within 36 to 72 hours depending on the classification of the cybersecurity Incident.

When making such a report to the authority, descriptions such as the time when the Incident occurs and when the agency becomes aware of the Incident, what had actually happened, the assessment of the risk level, the responsive measures that have been taken; the evaluation of any assistance from outside resources; and other relevant matters shall be included.

There are no specific provisions with regard to exemption of the reporting requirements, and it is not necessary for the authority to make such report publicly available.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There are no specific legal requirements in this regard. For non-government agencies that are not required under the Cybersecurity Management Act, they are encouraged to join other cybersecurity taskforces for information sharing, as long as such sharing does not constitute a breach of their confidentiality obligations. For example, they can participate in the reporting system and network maintained by TWCERT/CC.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

No. There are no such legal requirements under the Cybersecurity Management Act.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

If personal data is involved in a data breach Incident, pursuant to the PDPA, either a public agency or a non-public agency shall inform the affected data subjects of the data breach Incident as soon as it inspects the relevant Incident. In the notice to the data subjects, the relevant facts concerning the Incidents, such as what data was stolen, when the Incident happened, the potential suspect that breached the data, as well as the remedial actions that have been taken, shall be described. The PDPA does not set forth any threshold of the notification to the affected data subjects.

On the notification to the regulator, the PDPA does not specify any obligations to report a data breach Incident to the regulator. However, in the personal data security maintenance plans stipulated by the competent authorities of certain industries, the private sector is required to report a data breach Incident to the competent authority in charge of the industry. In most of the cases, the reporting will only become mandatory when the data breach Incident is deemed "material". Some of the competent authorities define the term "material" as "having the effect of affecting the daily operation" of the private business. The industries that shall report data breach Incidents to their regulators include online retailers and financial institutions, etc.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The sectoral regulators at the central government level in Taiwan are in charge of enforcing the relevant matters with regard to cybersecurity matters. With regard to personal data protection, either the sectoral regulators at the central government level or the municipal governments have the power to enforce the PDPA.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

With regard to cybersecurity, a private organisation that has been designated as a provider of the critical infrastructure may be ordered to take corrective measures by a certain deadline or it may be imposed with an administrative fine ranging from NTD100,000 to NTD1 million for its failure to comply with the obligations to (i) stipulate the relevant cybersecurity management plan, (ii) stipulate the responsive measures which should be taken in a cybersecurity Incident, or (iii) report the Incident to the relevant authority or submit the relevant investigation report, etc. and may be imposed with such fine consecutively until correction measures are taken.

With regard to a personal data breach Incident, if a private organisation fails to take proper security measures to protect the personal data that it retains or breaches its obligation to notify the data subjects affected by the personal data breach Incident, the competent authority has the power to order the private organisation to take corrective measures, and if no corrective measure is taken before the designated deadline, the authority has the power to impose an administrative fine ranging from NTD20,000 to NTD200,000 consecutively until corrective measures are made.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As the Cybersecurity Management Act was newly amended, thus far, no enforcement examples have been found. As for the PDPA, given that the enforcement power lies in the competent authority in charge of each different industry and there are no comprehensive methods to search such precedents, it is difficult to evaluate the level of the actual enforcement of each authority. The Financial Supervisory Commission (the "FSC"), however, has made the relevant enforcement decisions, which are online for public access. Based on the search in the FSC's database, there have been quite a few financial institutions being imposed with administrative fines for their failure to adopt proper security measures to protect the personal data that they retain or failure to notify the affected data subjects with regard to particular security Incidents.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are no specific laws, regulations or rulings in this regard. The general principles with regard to cybersecurity and computer crime under the relevant statutes such as those set forth in the Criminal Code as mentioned above will apply.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no specific laws, regulations or rulings in this regard. The general principles with regard to cybersecurity and computer crime under the relevant statutes such as those set forth in the Criminal Code as mentioned above will apply.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are no specific laws, regulations or rulings in this regard. The general principles with regard to cybersecurity and computer crime

under the relevant statutes such as those set forth in the Criminal Code as mentioned above will apply.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, different sectors implement different standards. For example, the regulators of the financial industry stipulate quite a few information security requirements and standards with specific security requirements, while the regulators of other industries may stipulate only general standards.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

With regard to the financial industry, there are various information security regulations and rulings requiring the financial institutions to take sufficient cybersecurity measures so as to protect their customers. For example, there are specific security standards for securities firms to offer "online" trading services to its customers, for banks to offer "online" banking services to their customers, and for insurance companies to offer insurance policies online.

As for the telecommunications sector, the competent authority, i.e., the NCC, also stipulates the relevant information security standards and measures and requires the telecommunications operators to adopt and follow the standards. The NCC also took certain measures to encourage telecommunications operators to maintain their information security, such as holding training sessions and seminars.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Directors bear "fiduciary duty" to the company and will be held liable when they breach such duty to the company. A company's failure to prevent, mitigate, manage or respond to an Incident may not necessarily lead to the conclusion that their directors have breached their fiduciary duty. Under Taiwanese law, directors are in charge of making business decisions for a company by forming the joint decision of the board, but they are not responsible for *implementing* any business decisions or the daily operation of the company. With regard to cybersecurity Incidents, it would depend on the internal rules of a company as to whether such an Incident shall be reported to the board of directors. If the management has reported an Incident to the board of directors pursuant to the internal rules, but the board of directors fails to take proper action to address or resolve the Incident or even try to conceal or cover the Incident, the board of directors may be held liable.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

It is not mandatory under Taiwanese law for a company to designate a CISO. Other than the specific non-government agency as designated by the relevant competent authority or the regulated companies, such as financial institutions or telecommunications operators, a company is not legally required to stipulate a written Incident response plan or policy, conduct periodical cyber risk assessments, or perform penetration tests or vulnerability assessments.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, unless such risks or Incidents are major or material to the operation of a listed company.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Not from the perspective of corporate governance.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In an Incident under which the computer system of a private organisation was hacked or invaded by others and the private organisation therefore suffered loss or damage, the private organisation, being the victim of the Incident, may file a civil lawsuit against the hacker or the other relevant wrongdoers either based on a tort claim or an unjustified enrichment claim, especially if there have been criminal proceedings launched against the hacker or the relevant wrongdoers at the same time. The private organisation, being the plaintiff, needs to establish the facts with regard to how the system was attacked, invaded or altered and how such activities can be linked to the hacker or the wrongdoers. The private organisation will also be required to substantiate the amount of the actual damage and the causation between the occurrence of the actual damage and the hacking activities.

Such a private organisation should also be able to file a civil action against the vendor that provided the IT/cybersecurity services to the private organisation if the vendor has failed to perform the required services or has failed to meet the required security standard. In this regard, the private organisation is required to establish that the vendor bears such an obligation to provide it with security service meeting a certain level or standard based on the relevant contract as well as substantiate the actual amount of the damage.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Since 2016, there have been quite a few "business email compromise" ("BEC") Incidents and many civil lawsuits were filed with the Taiwan court. Many of the cases involve a cross-border BEC scheme, under which a foreign company sought civil relief at the Taiwan court against individuals in Taiwan. Such individuals offered their bank accounts as the nominee accounts to receive the improper funds for the real hackers and their identities were discovered through the records in the banking system. The Taiwan law enforcement authority then worked with the foreign law enforcement authority to seize the nominee accounts and track down the individuals offering the nominee accounts. The nominee account holder would be held criminally liable under Taiwan law, either for being the accomplice of the hacker or breaching the Money Laundering Control Act. The victim would then bring a civil lawsuit against the nominee account holder. There are also court cases under which the nominee account holders were not found or criminally indicted but still the court ruled in favour of the victims against the nominee account holders and declared that the nominee account holders shall return the improper gain to the victims.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

The hackers invading or attacking others' systems will in general be liable under the tort law of Taiwan given that they may be deemed as (i) infringing other's rights, (ii) causing damage to others via a method that is against the good morals of Taiwanese society, or (iii) causing damage to others by breaching the statutes that are intending to protect others.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, they are permitted.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no such regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No. Monitoring employees is, in general, governed by the Communication Security and Surveillance Act, the privacy related law, and the PDPA. To conduct such monitoring, the employer shall ensure that the employees have been notified of such monitoring and have no "expectation" to their privacy with regard to the activities that the employer is monitoring.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No. Currently, a draft "whistle-blowing statute" bill is still pending.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

If the police suspect or become aware of a certain crime being conducted in relation to an Incident, the police have the power to conduct an investigation into the suspect by requiring the suspect or third party to provide the relevant "information" to the police. If the police intend to seize the hardware or devices, the police would need to prepare all collected evidence for the prosecutor and request the prosecutor to apply with the court for the issuance of a search warrant to seize the hardware or devices. The court will review the warrant application submitted by the prosecutor. If the evidence collected by the police meets the standard of probable cause, the court, in most cases, would issue the search warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such specific statutes under Taiwan law.

Ken-Ying Tseng established and currently heads Lee and Li's personal data protection practice group. Prior to 2018, she was the head of Lee and Li's M&A practice group for 12 years. She received an LL.M. from Harvard Law School. Ken-Ying advises on various forms of mergers and acquisitions, and is experienced in resolving both legal and commercial issues. She assisted and represented several multinational corporations in their M&A activities, including BASF, Henkel, Yahoo!, Arrow, Bureau Veritas, Aleees, Sony, Micrel, Energy Absolute, Qualcomm, McDonald's, among others.

In addition to M&A, Ken-Ying constantly advises various tech companies that are in the businesses of social networks, instant messengers, search engines, portal sites, sharing economy, e-commerce, OTT, online gaming, P2P lending, e-payments, cloud computing, and so on. Ken-Ying also frequently advises clients, including multinational companies, on privacy and data protection (GDPR), e-marketing, big data, e-signature, domain name, telecommunications, satellite, fintech, cybersecurity, Internet governance, and other legal issues.

Lee and Li, Attorneys-at-Law
8F, No.555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000
Email: kenying@leeandli.com
URL: www.leeandli.com

Lee and Li, Attorneys-at-Law is a full-service law firm and the largest law firm in Taiwan. Its history can be traced back to the 1940s. Lee and Li has formed practice groups which span corporate and investment, banking and capital markets, trademark and copyright, patent and technology, and litigation and ADR. Its services are performed by over 100 lawyers admitted in Taiwan and more than 100 technology experts, patent agents, patent attorneys, and trademark attorneys. Lee and Li was recognised as the 'Taiwan Firm of the Year' or the 'National Law Firm of the Year' by *IFLR* in 2001–2018. In 2019, for its professional and sophisticated legal practice in the field of mergers and acquisitions and financial and capital markets, Lee and Li is named the Most Innovative National Law Firm of the Year for Taiwan for 2019 by *IFLR*. Lee and Li has been recognised by other international institutions as the best law firm in the region, including, *Who's Who Legal*, *China Law & Practice*, *Leaders League*, *Chambers & Partners*, *Asialaw Regional Awards*, etc.

www.leeandli.com

Thailand

Supawat Srirungruang

Visitsak Arunsuratpakdee

R&T Asia (Thailand) Limited

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes. The Computer Crime Act B.E. 2550 (2007) ("**CCA**") provides that whoever illegally accesses a computer system that has specific security measures and such security measures are not intended for that person's use shall be liable to imprisonment not exceeding six months and/or a fine not exceeding THB 10,000. (CCA, s.5).

Whoever illegally accesses computer data that has specific security measures which are not intended for that person's use shall be liable to imprisonment not exceeding two years and/or a fine not exceeding THB 40,000. (CCA, s.7).

Denial-of-service attacks
Yes. Whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference to a computer system of another person so that it is not capable of functioning normally shall be liable to imprisonment not exceeding five years and/or a fine not exceeding THB 100,000. (CCA, s.10).

Phishing
Yes. Whoever dishonestly or deceitfully inputs into a computer system computer data which is distorted or forged, either in whole or in part, or computer data which is false, in such a manner likely to cause injury to the general public which is not the offence of defamation under the Criminal Code, shall be liable to imprisonment not exceeding five years and/or a fine not exceeding THB 100,000 (CCA, s.14(1)).

Where the offence above is not committed against the general public but rather against a person, the offender shall be liable to imprisonment not exceeding three years and/or a fine not exceeding THB 60,000; and such offence shall be deemed a compoundable offence.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes. In addition to the above, whoever illegally acts in a manner that damages, destroys, alters, amends, or makes additions to, either in whole or in part, computer data of another person shall be liable to imprisonment not exceeding five years and/or a fine not exceeding THB 100,000, or both. (CCA, s.9).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Yes. A person who distributes or disseminates a computer program created specifically for the purpose of committing offences specified shall be subject to imprisonment not exceeding two years and/or a fine not exceeding THB 40,000. Moreover, where there is a person who uses such computer program to commit an offence specified, the person who distributes or disseminates such computer program shall also be liable to a higher degree of penalty if he or she knew or might have been aware of the consequences that have occurred (CCA, s.13).

Identity theft or identity fraud (e.g. in connection with access devices)
Yes. Pursuant to Section 342(1) of the Criminal Code, identity theft/fraud would be considered as the offence of cheating and fraud committed by the offender showing himself or herself to be another person, and is subject to imprisonment not exceeding five years and/or a fine not exceeding THB 100,000, or both.

Section 269/5 also provides that whoever illegally uses the electronic card of another person in a manner likely to cause damage to other person(s) or people shall be liable to imprisonment not exceeding five years and/or a fine not exceeding THB 100,000, or both.

Identity theft/fraud would also be considered as the act of causing damage to the computer data of another person under the CCA (CCA, s.9). In addition, whoever inputs into a publicly accessible computer system computer data that will appear as an image of the other person and the image has been created, edited, appended or adapted by electronic means or whatsoever means, and in doing so is likely to cause such other person to be defamed, denounced, detested or humiliated, shall be liable to imprisonment not exceeding three years and/or a fine not exceeding THB 200,000 (CCA, S.16).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
There are no specific laws for electronic theft in Thailand. However, criminal copyright infringement usually constitutes an offence under the Copyright Act B.E. 2537 (1994).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Yes. Under the CCA, if a person who has knowledge of the security measures to access a computer system specifically created by another person illegally discloses such security measures in a manner that is likely to cause damage to another person, such person shall be liable to imprisonment not exceeding one year and/or a fine not exceeding THB 20,000 (CCA. s.6).

A person who illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilise would be liable to imprisonment not exceeding three years and/or a fine not exceeding THB 60,000 (CCA, s.8).

A person who sends computer data or an electronic mail to another person while hiding or faking its source(s), in a manner that interferes with such other person's normal utilisation of the computer system shall be liable to a fine not exceeding THB 100,000. Further, if the person sends computer data or electronic mail to another person in a manner that disturbs the recipient, without giving the recipient an easy opportunity to cancel or notify his/her wish to deny receipt of such computer data or electronic mails, such person shall be liable to a fine not exceeding THB 200,000 (CCA, s.11).

In case the commission of the above offences is associated with computer data or a computer system that relates to national security and safety, public security, economic security or infrastructure which is for the public interest, the offender shall be liable to imprisonment for up to 15 years and a fine for up to THB 300,000 (CCA, s.12).

In addition, a person who inputs into a computer system: (i) false computer data in a manner which is likely to cause damage to the protection of national security, public safety, economic security or infrastructure which is for the public interest or to cause panic to the general public; or (ii) computer data which is an offence related to national security or terrorism under the Criminal Code, shall be liable to imprisonment not exceeding five years and/or THB 100,000 (CCA, ss.14(2)–(3)).

Failure by an organisation to implement cybersecurity measures

Yes. Under the CCA, any service provider who cooperates, consents to or acquiesces in the commission of an offence under Section 14 with regards to a computer system in his control would be liable to the same penalty (CCA, ss.14–15).

The newly enacted laws (i.e. Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") and the Cybersecurity Act B.E. 2562 (2019) ("**Cybersecurity Act**")) also impose obligations on cybersecurity measures for organisations.

Under the PDPA, the data controller shall provide appropriate security measures for preventing the unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data, and such measures must be reviewed when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate security and safety (PDPA, s.37). Likewise, the data processor shall provide appropriate security measures for preventing unauthorised or unlawful loss, access to, use, alteration, correction or disclosure, of personal data, and notify the data controller of the personal data breach that occurred (PDPA, ss.40(2)). The data controller and/or data processor who fails to comply without appropriate reasons shall be liable to an administrative fine not exceeding THB three million (PDPA, ss.83 and 86).

The Cybersecurity Act provides that, in the event of a cyber threat significantly occurring to the system of the Organization of Critical Information Infrastructure ("**CII Organization**"), the CII Organization shall report to the Office of the National Cybersecurity Committee ("**Office**") and the supervising or regulating organisation, and cope with the cyber threats. A CII Organization that fails to report a cyber threat Incident without reasonable cause shall be subject to a fine not exceeding THB 200,000 (Cybersecurity Act, s.57).

1.2 Do any of the above-mentioned offences have extraterritorial application?

Generally, under the Criminal Code, where the criminal offence relating to public security, cheating or fraud is committed outside Thailand and (i) the offender is a Thai national and there is a request for punishment by the government of the country where the offence has occurred or by the injured person, or (ii) the offender is a non-Thai national and the Thai Government or a Thai person is an injured person and there is a request for punishment by the injured person, the offender could be punished under the laws of Thailand.

The PDPA applies to the collection, use, or disclosure of personal data by a data controller or a data processor that is in Thailand, regardless of whether such collection, use, or disclosure takes place in Thailand or not. Where a data controller or a data processor is outside Thailand, the PDPA shall apply to the collection, use, or disclosure of personal data of data subjects who are in Thailand, provided that the activities of such data controller or data processor are the following activities:

(1) the offering of goods or services to the data subjects who are in Thailand, irrespective of whether the payment is made by the data subject; and
(2) the monitoring of the data subject's behaviour, where the behaviour takes place in Thailand. (PDPA, s.5).

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes. There is an exception which applies only to service providers for the offences under Sections 14–15 of the Cybersecurity Act. Where the service provider is able to prove it has complied with the Ministerial Notification setting out procedures for the notification and suppression of the dissemination of such data and the removal of such data from the computer system, it would be exempt from the penalty (Cybersecurity Act, s.15).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Yes. Section 269/4 of the Criminal Code provides that whoever uses or acquires for use an electromagnetic record/electronic card which is forged or altered in accordance with Section 269/1 shall be liable to imprisonment of between one and 10 years or to a fine of THB 20,000 to THB 200,000, or both. For example, three men were accused of conspiring to hack and forge electronic card information in the systems of a telecommunications operator to raise the cards' top-up value to THB 105,000,000 and then selling them for THB 12,000,000. They were found guilty of selling forged electronic cards and were imprisoned.

Section 135/1 (2) of the Criminal Code provides that whoever commits any act to cause serious injury to a transportation system, communication system or infrastructure which is for public interest with the aim being to threaten or force the Thai Government, a Foreign Government or international organisation to perform or not to perform any act which may cause serious injury, or with the aim of creating disorder by causing people to be terrified, such person commits an offence of terrorisation and shall be punished with death, imprisonment for life or imprisonment from three years to 20 years and a fine ranging from THB 60,000 to 1,000,000.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- Section 32 of the Constitution of the Kingdom of Thailand.
- Criminal Code.
- CCA.
- Cybersecurity Act.
- PDPA.
- Electronic Transactions Act B.E. 2544 (2001), as amended.
- Special Case Investigation Act B.E. 2547 (2004), as amended.
- Telecommunications Business Act B.E. 2544 (2011), as amended ("**TBA**").
- Payment Systems Act B.E. 2560 (2017) ("**Payment Systems Act**").
- The National Council for Peace and Order Announcements.
- The Royal Decree prescribing Criteria and Procedures for Electronic Transactions of the Government Sector B.E. 2549 (2006).
- The Royal Decree on Security Procedures for Electronic Transactions B.E. 2553 (2010).
- The Notifications issued by the Electronic Transactions Commission ("**ETC**").

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Yes. According to Section 49 of the Cybersecurity Act, the National Cybersecurity Committee has the power to prescribe the characteristics of the organisations that have missions or provide services in the following aspects to be the CII Organization:

(1) national security;
(2) substantive public service;
(3) banking and finance;
(4) information technology and telecommunications;
(5) transportation and logistics;
(6) energy and public utilities;
(7) public health; or
(8) other as prescribed by the National Cybersecurity Committee.

The CII Organization has obligations under the Cybersecurity Act, such as taking actions in accordance with the National Cybersecurity Committee's policy and plans for maintaining cybersecurity, preparing its code of practice and standard framework, and preventing and mitigating risks from cyber threats.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Under the Cybersecurity Act, the CII Organization has the duty to conduct risk assessment on maintaining cybersecurity and to establish a mechanism or process to monitor cyber threats or cybersecurity Incidents which relates to its critical information infrastructure and shall participate in assessment of the readiness in coping with cyber threats as held by the Office (Cybersecurity Act, ss.54–56).

Under the PDPA, the organisation which is the data controller or the data processor also required to take measures to monitor, detect, prevent or mitigate Incidents. (Please see also our comments in question 1.1.)

Additionally, specific requirements may also apply to organisations in specific industries; for example, Section 50 of the TBA and the notification issued thereof, the telecommunication licensee shall put in place protection and security measures pertaining to personal data both in technical and internal organisational management aspects suitable with each type of telecommunications services.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No, there are no conflict of laws issues.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. Section 57 of the Cybersecurity Act requires the CII Organization to report any event of a cyber threat significantly occurring to its system to the Office and the supervising or regulating organisation. The Cybersecurity Regulating Committee ("**CRC**") may prescribe criteria and methods for reporting in the future.

Section 37(4) of the PDPA provides that the data controller shall notify the Office of the Personal Data Protection Committee of any personal data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such personal data breach is unlikely to result in a risk to the rights and freedoms of the persons. The notification and the exemption to the notification shall be made in accordance with the rules and procedures set forth by the Personal Data Protection Committee. There is, however, currently no such rules and procedures announced.

Sectoral laws also impose reporting obligations on specific industries. For example, under the Payment Systems Act, e-payment service providers are required to notify the Bank of Thailand ("**BOT**") of an occurrence of any problem or failure to provide e-payment service as soon as possible, regardless of whether such problem/failure is caused by the occurrence of an Incident. Under

the Securities and Exchange Act 1992 ("**SEA**"), securities companies are required to notify, either by verbal or electronic means, the Securities and Exchange Commission ("**SEC**") without delay upon the acknowledgment of a system disruption, unauthorised access to a system or an Incident that results in damage to the security company's reputation, such as website defacement.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Please see our comments in question 2.5 above.

There are no legal provisions prohibiting or restricting organisations from notifying foreign authorities or private sector organisations.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes. Section 37(4) of the PDPA provides that, if the personal data breach is likely to result in a high risk to the rights and freedoms of persons, the data controller shall also notify the data subject of the personal data breach and remedial measures without delay.

The notification shall be made in accordance with the rules and procedures set forth by the Personal Data Protection Committee. There is, however, currently no such rules and procedures announced.

Specific reporting obligations apply to the securities companies under the SEA, and the telecommunication licensee under the TBA.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No. The responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

(a) Cybersecurity Regulating Committee ("**CRC**").
(b) Personal Data Protection Committee ("**PDPC**").
(c) National Broadcasting and Telecommunications Commission ("**NBTC**").
(d) Bank of Thailand ("**BOT**").
(e) The Securities and Exchange Commission ("**SEC**").
(f) A police officer – the official who has the authority to initiate an investigation or proceedings relating to a criminal offence, including CCA offences.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

(a) Under the Cybersecurity Act, the CII Organization that fails to report a cyber threat Incident without reasonable cause would be subject to a fine not exceeding THB 200,000.
(b) Under the PDPA, the penalty for data controller/data processor not complying with the notice requirements under questions 2.3, 2.5 and 2.7 is an administrative fine not exceeding THB 3,000,000.
(c) Under the SEA, the penalty for securities companies not complying with the notice requirements under questions 2.5 and 2.7 is a fine not exceeding THB 300,000 and a further fine not exceeding THB 10,000 for every day during which the violation continues. The director, manager or any person responsible for the operation of such securities company shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding THB 200,000, or both, unless it can be proven that such person has no involvement with the commission of the offence by such securities company.
(d) With respect to e-payment service providers under the supervision of the BOT, the penalty for not complying with the notice requirement under question 2.5 is a fine not exceeding THB 1,000,000 or THB 2,000,000 depending on the type of e-payment service providers.
(e) If the Licensee under the TBA fails to comply with the requirement identified under question 2.3 or the prescribed licensing conditions, the NBTC has the power to order the Licensee to: refrain from carrying out the violating act(s); carry out rectification and improvement; or perform actions correctly or appropriately within a specified period of time. If the Licensee fails to comply with the order, the Licensee shall be liable to an administrative fine of not less than THB 20,000 per day and in case the Licensee still fails to perform the actions correctly, or where there is serious damage to the public interest, the NBTC has the power to suspend or revoke the licence.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In 2018, according to media reports, the personal data of around 46,000 users of TrueMove H, Thailand's mobile operator, was leaked into Amazon Web Services' ("**AWS**") cloud storage and the NBTC ordered TrueMove H to solve the Incident and report the result to the NBTC.

We found no other non-compliance cases taken by the relevant regulators which have been announced to the public.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Not applicable. According to Section 60 of the Cybersecurity Act, the Office is entitled to determine the measures to prevent, cope

with, assess, suppress and suspend the cyber threats in each level. As of now, there is no notification regulating the use of Beacons to detect and deflect Incidents in Thailand.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Please see the comment provided with regard to Beacons above.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Please see the comment provided with regard to Beacons above.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. Based on Section 50 of the TBA and the notification issued thereof, the Licensee shall put in place protection and security measures pertaining to personal data both in technical and internal organisational management aspects suitable with each type of telecommunications services. The protection and security measures pertaining to personal data in a technical aspect shall be undertaken at least as follows:

(1) the encoding and decoding system which is used to maintain the security of personal data shall be modified at least every three months; and
(2) the level of safety system shall be adjusted suitably in alignment with the risks arising due to technological advancement.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes.

(a) Financial services sector: organisations which operate e-payment services are regulated under the relevant BOT notifications. E-payment service providers are required to have a contingency plan or a backup system for the purposes of continuity of the service and a safety policy or measures for the information system, which must at least meet the standards prescribed in the BOT notifications. Moreover, e-payment service providers are required to keep customer data confidential throughout and after the use of its services, with certain exceptions.
(b) Telecommunications sector: the telecommunications sector is administrated by the NBTC. The NBTC has issued notifications setting out rules and procedures for the management of information technology, and procedures for protecting personal information, rights of privacy and freedom in communication through telecommunications' means. Please see details in our comments in question 3.1 above. Moreover, the NBTC has the power to prescribe specific provisions concerning cybersecurity to each licensed telecommunication operator.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Yes. It is not unusual in Thailand for third parties to sue directors together with the company for the alleged commission of offences.

Some laws also provide specific provisions on director liability. According to Section 77 of the Cybersecurity Act and Section 81 of the PDPA, where the offence was committed by a company as the result of an order, an act or omission to order or act, by a director, such director must be liable to the penalties prescribed for such offence.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) No. There is no requirement regarding CISO under the current Applicable Laws. However, as at the time of writing, the draft BOT Notification Re: Regulations on Information Technology Risk of Financial Institutions, which contains a requirement for domestic systemically important banks to designate a CISO (chief information security officer), is in the process of conducting a public hearing.
(b) Yes. Section 44 of the Cybersecurity Act requires the CII Organization to prepare a code of practice and standard framework for maintaining cybersecurity which shall comprise the plan for examining and assessing risks related to maintaining cybersecurity, as well as, the plan for coping with the Incidents. Also generally under the PDPA, data controllers and data processors shall provide appropriate security measures for preventing the unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data which must be in accordance with the minimum standard specified and announced by the Personal Data Protection Committee.
(c) Yes. Section 54 of the Cybersecurity Act requires the CII Organization to conduct risk assessment on maintaining cybersecurity by having an examiner, including examination in the cybersecurity aspect by the information security auditor, internal auditor or external independent auditor, at least once per year.
(d) Yes. Section 56 of the Cybersecurity Act requires the CII Organization to participate in the assessment on the readiness in coping with the Incidents as held by the Office.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Please see our comments in questions 2.5 and 2.7 above.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Yes. Securities companies are required to submit an annual report which includes its IT management and occurrence of Incidents to the SEC. E-payment service providers are also required to prepare information and details as to the provision of services and make the same available for inspection by the BOT. The BOT has the power to instruct an e-payment service provider to provide any information in relation to its services, including information on the occurrence of Incidents.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Where the data controller or the data processor violates or fails to comply with the PDPA which causes damage to the data subject, the party in breach is bound to compensate the data subject for damages suffered, regardless of whether such operation is performed intentionally or negligently.

Apart from actual compensation, the Court may order the party in breach to pay punitive damages as the court deems fit, but not exceeding two times the actual compensation amount.

In addition, issues relating to Incidents are generally governed by the Civil and Commercial Code ("**CCC**") under the section relating to a "wrongful act" (i.e., Section 420 of the CCC). If any Incident, whether wilfully or negligently, unlawfully damages or injures another person's life, body, health, liberty, property or any right, the party in breach is said to have committed a wrongful act and is bound to pay compensation for damages suffered. The general guidance from Thailand's Supreme Court decisions is that the injured party is entitled to claim actual damage suffered, with the burden of proof being on the claimant.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

In 2016, the accused was arrested in connection with the attacks that caused some government websites to be blocked and non-public files to be leaked. The legal status of the accused and the progress of the case are not yet available to the public.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Please see our comment in question 5.1 above.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, there are no regulatory limitations for the organisations to take out insurance against Incidents in Thailand.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No, there are no specific requirements under Applicable Law. However, we noted that the Cybersecurity Act and PDPA is awaiting the issuance of implementing regulations, which may include these topics.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are no Applicable Laws that may prohibit or limit the reporting of the above.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In coping with and to remedy damage from a cyber threat at a critical level, the CRC has the power to order any relevant person to: (i) monitor the computer or computer system; (ii) examine the computer or computer system to find an error, analyse the situation, and evaluate the effects from the cyber threat; (iii) conduct a measure rectifying the cyber threat; (iv) maintain the status of the computer data or computer system to operate the computer forensic science; and (v) provide access to the relevant computer data or other information related to the computer system.

CRC also has the power to order a competent official to do the following: (i) enter into a place to examine; (ii) access the computer data, computer system or other data, copy, or filter/screen information data or computer program; (iii) test the operation of the computer or computer system; and (iv) seize or freeze a computer, a computer system, or any equipment.

For the benefit of an investigation, if there is reasonable cause to believe that there is the commission of an offence under the CCA, or there is a request by the inquiry official, the competent official is empowered to acquire evidence to prove an offence and to identify the accused, for example, by: (i) issuing an inquiry letter to any person related to the commission of an offence to give statements, forward written explanations or any other documents, data or

evidence in a comprehensible form; (ii) requiring computer traffic data related to communications from a service user via a computer system or from other relevant persons; (iii) instructing a service provider to (a) deliver user-related data that is required to be retained under the CCA requirements or that is in the service provider's possession or control to the competent official, or (b) keep the data for later; or (iv) seizing or attaching a computer system for the purposes of obtaining details of the offence and the person who committed the offence.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes. In relation to criminal offences in violation of the CCA or any other laws committed against any persons by using a computer system, computer data or equipment storing computer data, which is a composition or part of the commission of the offence or has computer data relating to a commission of any offence under another law, the competent official is empowered to decrypt any person's computer data or order a person related to the encryption of the computer data to decrypt it, or cooperate with the competent official to decrypt it.

Supawat Srirungruang is a Partner in the Corporate & Commercial Practice of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann Asia. Supawat graduated with a Bachelor of Laws (with honours) from Thammasat University (1998), and has a Master of Laws from California Western School of Law (2001) and University of Sydney (2002). Prior to joining Rajah & Tann, Supawat spent more than 14 years working for leading American- and Australian-based international law firms in Thailand. Supawat focuses his practice on technology, media & telecommunications matters, regulatory compliance, administrative law, dispute resolution, anti-bribery, competition law, labour law issues, merger and acquisitions, customs regulation, project development, and international trade laws.

R&T Asia (Thailand) Limited
973 President Tower, 12th Floor Units 12A–12F
Ploenchit Road, Lumpini, Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Email: supawat.s@rajahtann.com
URL: www.rajahtannasia.com

Visitsak Arunsuratpakdee is a Partner in the Corporate & Commercial Practice of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann Asia. Visitsak focuses his practice on regulatory compliance, mergers and acquisitions, capital markets, litigation, taxation and general corporate matters. Arising out of his work for energy and telecommunications companies in various matters and concession-related disputes, Visitsak has also expanded his practice to include disputes with government agencies over the terms of concessions and administrative decision-making. Visitsak advises foreign and Thai multinational clients on regulatory compliance in their business operations and has represented them in various cases. He has also represented both private clients and Thai governmental authorities in relation to corporatisation, privatisation, business reorganisation and infrastructure projects.

R&T Asia (Thailand) Limited
973 President Tower, 12th Floor Units 12A–12F
Ploenchit Road, Lumpini, Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Fax: +66 2656 0833
Email: visitsak.a@rajahtann.com
URL: www.rajahtannasia.com

R&T Asia (Thailand) Limited, based in Bangkok, has an impressive base of international, regional and local clients.

We have many years of experience in advising on a range of Thai law matters, including representing clients in civil, criminal or administrative proceedings, international and domestic arbitration, government investigations and compliance proceedings, structuring foreign direct investment and mergers and acquisitions involving private or listed companies, and general corporate commercial matters for foreign investors in Thailand.

The team has a particular expertise in representing clients in highly regulated industries, such as oil & gas, petrochemical, telecoms, tobacco, food & beverage, insurance and manufacturing, and can provide full support in large-scale litigation, transactions and investigations.

The team comprises a majority of Thai nationals who are qualified to advise on Thai law. Our Thai lawyers are fluent in Thai and English and are fully conversant with the practical application of the law within Thailand's business and cultural landscapes.

www.rajahtannasia.com

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

USA

Ropes & Gray


Edward R. McNicholas


Kevin J. Angle

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

The federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is the primary statutory mechanism for prosecuting cybercrime, and provides for both criminal and civil penalties. The CFAA prohibits: (1) unauthorised access (or exceeding authorised access) to a computer and obtaining national security information; (2) unauthorised access (or exceeding authorised access) to a computer that is used in interstate or foreign commerce and obtaining information; (3) unauthorised access to a non-public computer used by the United States government; (4) knowingly accessing a protected computer without authorisation with the intent to defraud; (5) damaging a computer either intentionally or recklessly; (6) trafficking in passwords; (7) transmitting threats of extortion, specifically threats to damage a protected computer and threats to obtain information or compromise the confidentiality of information; and (8) cyber-extortion related to demands of money or property. Depending on the specific offence, penalties can range from one to 20 years in prison.

Other relevant laws include the Electronic Communications Protection Act ("ECPA"), which provides protections for communications in storage and in transit. Under the Stored Communications Act (Title II of the ECPA), 18 U.S.C. § 2702, it is a criminal violation to intentionally access without authorisation (or exceed authorised access) a facility that provides an electronic communications service ("ECS"), which could include, among others, email service providers or even employers who provide email addresses to their employees. Personal computers are not considered facilities providing an ECS. Violations are subject to penalties ranging from up to one year for first time violations without an improper purpose (i.e., violations that are not committed for commercial advantage, to cause malicious destruction or damage or the like) to up to 10 years for repeat violations for an improper purpose. Intentionally intercepting electronic communications in transit is prohibited by the Wiretap Act (Title I of the ECPA), 18 U.S.C. § 2511, with exceptions for law enforcement, some service providers and others (including, potentially, employers). Penalties for violations can include imprisonment for up to five years.

The CAN-SPAM Act prohibits certain activities related to spam email, including accessing a computer to send spam emails without authorisation and using false information to register for multiple email addresses to send spam emails. Penalties for violations can be up to three years' imprisonment.

In addition to federal statutes, numerous states have passed statutes prohibiting hacking and other computer crimes, some of which are broader than the federal statute. New York, for example, prohibits the knowing use of a computer with the intention to gain access to computer material (computer trespass), N.Y. Penal Law § 156.10, with penalties of up to four years' imprisonment, and knowing unauthorised use of a computer, N.Y. Penal Law § 156.05, 156.20 *et seq.*, with penalties of varying ranges up to 15 years' imprisonment, depending on the severity of the offence. New York is merely one example; dozens of such state laws exist. The specification of which statute is applicable depends on several factors.

Hacking (i.e. unauthorised access)
Yes, hacking could violate, among other statutes, the CFAA, 18 U.S.C. § 1030(a)(1) (national security information, imprisonment up to 10 years), (2) (obtaining information, imprisonment up to one year, or five if aggravating factors apply), (3) (government computers, imprisonment up to one year) and (4) (accessing to defraud, imprisonment up to five years).

Denial-of-service attacks
Yes, a DOS attack could violate CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission, imprisonment up to 10 years), as well as state computer crime laws.

Phishing
Yes, among other statutes, phishing could violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) or constitute wire fraud under 18 U.S.C. § 2702, which carries a potential sentence of up to 20 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes, planting malware would violate CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission, imprisonment up to 10 years), as well as state computer crime laws.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Mere possession of hacking tools would be difficult to prosecute in the absence of intent to use them for illegal purposes. If there were evidence of criminal intent and some overt act taken towards that end, a person may be liable for an attempt to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), or related computer crimes laws. With respect to federal statutes, attempt is subject to the same sentence as commission of the offence.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes, identity theft could be charged under the federal identity theft statute, 18 U.S.C. § 1028, as well as numerous state laws.

Electronic theft (e.g., breach of confidence by a current or former employee, or criminal copyright infringement)
Yes, electronic theft could violate CFAA, 18 U.S.C. § 1030(a)(2) (obtaining information, imprisonment of up to one year, or five if aggravating factors apply). It may also, or alternatively, violate the Economic Espionage Act, 18 U.S.C. § 1831–1839, which creates two crimes based on the theft of trade secrets; the first makes it a crime to acquire, without authorization, trade secrets in order to benefit a foreign government, and the second if the theft will create economic benefit for others and will injure the target of the theft.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
The CFAA, 18 U.S.C. § 1030(a)(2), and wire fraud statute, 18 U.S.C. § 2702, as well as numerous state laws apply to a wide variety of criminal conduct online.

Failure by an organisation to implement cybersecurity measures
Failure to implement cybersecurity measures would not normally arise to a criminal violation, although it is possible for certain regulated entities. Organizations would likely face regulatory scrutiny and potential civil actions in the event their failure to implement cybersecurity controls results in a data breach.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the USA PATRIOT Act amended the CFAA and Access Device Fraud statute, 18 U.S.C. § 1029, to expressly apply them extraterritorially.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The existence of a robust corporate compliance program, as well as cooperation with law enforcement, may help to mitigate any penalty or influence prosecutorial discretion. The nature of the crime, whether it was intentional or unintentional, whether it was committed for economic benefit or malice and the number of past offences may also impact the severity of any penalty.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Yes. Among others, the federal Wire Fraud Statute, 18 U.S.C. § 1343, is a common tool for prosecuting a variety of fraudulent online activity, including hacking and other cybercrimes. The statute prohibits the use of wires in interstate commerce for the purpose of executing a scheme or artifice to defraud. It has been used to prosecute, among others, the alleged hacker in the recent Capital One data breach, *United States of America v. Paige Thompson*, CR19-159, in which the hacker was accused of executing a scheme to defraud by exploiting firewall misconfigurations to access personal information and steal cryptocurrency.

Other offences that may arise in relation to an Incident include:

Identity Theft, 18 U.S.C. § 1028, which criminalises conduct involving fraudulent identity documents or the unlawful use of identity information. It was used in *United States v. Sutcliffe*, 505 F.3d 944 (9th Cir. 2007), to prosecute an individual for posting stolen social security numbers to a website.

Access Device Fraud, 18 U.S.C. § 1029, which criminalises various conduct involving unauthorised uses of "access devices", such as credit card numbers or bank account information to conduct monetary transactions. It has been used to prosecute individuals in phishing campaigns, among others.

National Stolen Property Act, 18 U.S.C. § 2314, which prohibits the transport in interstate commerce of stolen goods or wares, money or articles used in counterfeiting whose value exceeds $5,000. Among other possible applications, it has been used to prosecute fraudulently induced wire transfers, although attempts to utilise the act to prosecute individuals based on the theft of source code have met resistance because the source code form has not been deemed to be a "tangible item", and therefore not a "good or ware". *E.g., United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012).

Other laws of more general applicability, such as laws regarding securities fraud (in the event stolen information is used to trade on the securities markets) and others, may also apply. Each state may also have a variety of statutes that criminalise fraud, wire fraud, bank fraud, possession of stolen property and related conspiracies.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Numerous federal and state laws include cybersecurity requirements. The Federal Trade Commission ("FTC") has been particularly active in this space and has interpreted its enforcement authority under Section 5(a) of the FTC Act, applying to unfair and deceptive practices, as a means to require companies to implement security measures. Since 2002, the FTC has brought more than 65 enforcement actions against companies it alleges failed to implement reasonable security measures.

Some federal laws, however, are sector-specific or extend only to public companies. For example, the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations require "financial institutions" to implement written policies and procedures that are "reasonably designed" to ensure the security and confidentiality of customer records, and protect against anticipated threats and unauthorised access and use. The Health Insurance Portability and Accountability Act ("HIPAA") includes cybersecurity requirements applicable to protected health information in the possession of certain "covered entities" and their "business associates".

At the state level, several states have passed laws imposing security requirements. Most of these statutes require some form of "reasonable security". Massachusetts regulations impose specific security requirements on companies that own or license personal information, including the implementation of a written security program and encryption of data in transit across public networks and on all portable devices. New York recently passed its SHIELD Act, requiring reasonable security for personal information and specifying specific measures that may satisfy that standard. The California Consumer Privacy Act creates a data breach right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove that the impacted business failed to implement and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect the personal information.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Cybersecurity and Infrastructure Security Agency ("CISA") Act created CISA, a component of the Department of Homeland Security, and the federal agency responsible for protecting critical infrastructure in the United States. CISA coordinates between government and private sector organisations in protecting critical infrastructure. The federal government has issued sector-specific guidance for critical infrastructure operators and the nuclear, chemical, electrical, government contracting, transportation and other sectors have detailed statutory and regulatory requirements.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Generally, yes. U.S. cybersecurity laws exist at both the federal and state levels and vary by commercial sectors. For instance, several federal statutes have data breach notice provisions, but each state and four territories also have data breach laws. Many regulators expect regulated companies to have implemented "reasonable" security measures, taking into account factors such as the sensitivity of the data protected. In light of the proliferation of standards, many companies rely on omnibus cybersecurity frameworks like the NIST Cybersecurity Framework, which recommends that companies take steps to identify and assess material foreseeable risks (including with vendors), design and implement policies and controls to protect the organisation in light of those risks, monitor for and detect anomalies and realised risks, respond promptly and adequately to Incidents and then recover from any Incident.

In addition to general reasonable security requirements, some U.S. laws are much more prescriptive. For example, Massachusetts and New York have detailed information security requirements at the state level, and the New York Department of Financial Services (which regulates entities such as banks and insurance companies) has further additional requirements.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Laws and regulations regarding cybersecurity have been passed at the federal level and in all 50 states. Federal laws will always trump inconsistent state laws, but states can frequently provide more and different protections than the federal laws. Conflicts are resolved by an analysis of whether the federal standards preempt the state requirements in particular circumstances and by analysis of the jurisdiction of a particular federal agency or state over the parties and controversies at issue.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, all states and four territories have requirements for the reporting of Incidents and most of these statutes require reporting to state regulators . The nature and scope of the information that is required to be reported varies. For example, Massachusetts requires that organisations reporting a breach to state regulators must include information about (i) the nature of the breach of security or unauthorised acquisition or use, (ii) the number of residents of Massachusetts affected by the Incident, (iii) any steps taken to address the Incident, (iv) the name of the organisation reporting and experiencing the breach, (v) the person responsible, if known, (vi) the type of personal information potentially compromised, (vii) whether the organisation maintained a written information security program, as required by Massachusetts regulations, and (viii) whether the organisation is updating that program in response to the Incident.

These state requirements are in addition to federal requirements that are sector-specific. For example, the Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") requires covered entities and business associates to report certain Incidents involving Protected Health Information ("PHI").

Timeframes for reporting vary by state or agency, with most requiring notification around the same time that individuals are notified (or sometimes in advance). Vermont requires any notification to its Attorney General to be sent within 15 days. Covered financial institutions are required to report breaches to the New York Department of Financial Services within 72 hours. At the request of law enforcement agencies, however, some notifications may be delayed.

Information about cyber threats generally need not be reported.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Yes, organisations are encouraged to report threat information. The federal Cybersecurity Act of 2015, also known as the Cybersecurity Information Sharing Act ("CISA"), provides that, notwithstanding any other provision of law, organisations may share cyber threat indicators or defensive measures. The CISA also provides that such sharing does not waive applicable privileges such as the attorney-client privilege.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

All 50 U.S. states and four territories have now passed breach notification statutes with varying requirements. Typically, breach notification statutes require notification be sent to individuals whose electronic Personal Information, as defined therein, was acquired in an Incident; though some states require notification based on access to such information alone. State definitions of Personal Information triggering data breach notification generally apply to the first name or first initial and last name in combination with another identifier, when not encrypted or redacted, such as social security number, driver's licence or identification card number, or account number, or credit card or debit card number in combination with any required security code, access code or password that would permit access to the individual's account. Increasingly, states are also including in the definition of Personal Information, health and biometric information, as well as usernames and passwords that provide access to an online account. Many states also require notice be sent to Attorney Generals or other state agencies, often depending on the number of individuals impacted. Most states allow for consideration of whether there is a risk of harm to the data subjects, but some states do not allow for such consideration.

Timeframes for notification vary by state. Florida and Colorado currently require notification to individuals be sent within 30 days.

Additionally, some sector-specific laws provide notification requirements. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA-covered entities and business associates to provide notifications in the event of certain Incidents impacting protected health information ("PHI").

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Notification requirements typically do not require this information in the first instance, but law enforcement may subsequently request it. Organisations need to carefully balance their obligations under Applicable Laws with the requests emanating from law enforcement. The Cybersecurity Information Sharing Act does provide some protection with respect to cybersecurity threat indictors or defensive measures.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The regulator varies by sector, law and state. The FTC is the principal U.S. federal privacy regulator covering most for-profit businesses not overseen by other regulators. The SEC regulates many financial institutions and the OCR is primarily responsible for enforcing HIPAA. State Attorney Generals have broad authority regarding enforcement of cybersecurity matters. In addition, federal and state regulators in particular sectors, such as insurance, have further enforcement powers.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

The U.S. has no single framework for non-compliance with notice requirements and penalties will depend heavily on the relevant law and regulator. In addition to regulatory penalties, private plaintiffs may file actions alleging non-compliance with relevant laws. For example, the California Consumer Privacy Act provides for statutory damages of between $100 to $750 per consumer and per Incident in the event of a data breach caused by the failure to have in place reasonable security measures.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Hundreds of actions have been brought for non-compliance. For instance, Equifax agreed to pay at least $575 million as part of a settlement with the FTC, CFPB and 50 U.S. state Attorney Generals, or other state regulators charged with overseeing data security, related to its 2017 data breach allegedly impacting approximately 147 million people. Government authorities alleged that Equifax failed to have in place reasonable security for the information it collected and stored.

Typical of the FTC's enforcement is a case involving Uber in which it entered into an expanded settlement with Uber arising from a 2016 data breach, which the FTC alleged was not disclosed to the FTC for more than a year. The FTC had previously settled allegations related to an earlier 2014 breach. The FTC had alleged that Uber failed to live up to statements that access to rider and driver accounts were closely monitored, which, the FTC alleged, was not the case, rendering the statements false or misleading.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e., imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Generally, yes.

Honeypots (i.e., digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Generally, yes.

Sinkholes (i.e., measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Generally, yes.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Cybersecurity laws in the United States vary significantly by business sector. There is currently no single U.S. cybersecurity law of general application other than, arguably, restrictions of "unfair" trade practices. Most businesses must comply with sector-specific federal and states laws. Healthcare organisations, for example, may need to comply with the Health Information Portability and Accountability Act ("HIPAA"), and many financial institutions are required to comply with the Gramm-Leach-Bliley Act ("GLBA"). Related state laws impose additional requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial Services: Financial services organisations must comply with the GLBA and its implementing regulations (which vary depending on the organisation's functional regulator). The SEC, other regulators and industry groups, such as FINRA and the NFA, have published cybersecurity guidance that should be carefully reviewed. Red Flag Rules published by regulators require covered firms to adopt written programs to detect, prevent and mitigate identity theft. The Fair Credit Reporting Act ("FCRA") and Fair and Accurate Credit Transactions Act ("FACTA") impose requirements with respect to credit reports. The FTC's Disposal Rule, 16 C.F.R. § 682, issued pursuant to FACTA, requires certain practices for the destruction of certain information contained in or derived from a credit report. State regulators sometimes impose very significant further regulations, particularly in New York.

Telecommunications: The Communications Act, as enforced by Federal Communications Commission ("FCC") regulations, requires telecommunications carriers and providers of Voice over Internet Protocol ("VoIP") services to protect "customer proprietary network information". Substantial fines and penalties can be assessed for failure to ensure adequate protections.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

Public company boards of directors owe shareholders fiduciary duties, including the duties of care and loyalty. To fulfill these duties, among other things, boards must ensure that they are properly informed regarding the company's cybersecurity risks and the efforts the company has made to address them.

In the event of an Incident, boards may face scrutiny and potentially litigation relating to their oversight of the company's cybersecurity. For example, in the Yahoo! data breach, individual board members faced a shareholder derivative action alleging that they failed to exercise their fiduciary duties, failed to ensure that proper security measures were in place, failed to adequately investigate the Incident and made misleading statements. The allegations were ultimately settled for a reported $29 million. In that same Incident, the Securities and Exchange Commission issued a $35 million fine.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Federal and state laws may impose specific cybersecurity requirements that depend on the entity's functional regulator and the residence of the data subject. For example, the New York Department of Financial Services has issued regulations requiring covered financial institutions (which include banks and insurance companies) to, among other things, designate a CISO, establish a written Incident response plan and conduct a periodic risk assessment, annual penetration testing and bi-annual vulnerability assessments. Massachusetts information security regulations, likewise, require organisations that collect certain Personal Information from Massachusetts residents to implement a comprehensive information security program that, among other things, identifies and assesses reasonably foreseeable internal and external risks to the security, confidentiality and integrity of such information. While not expressly required by regulation, the Securities and Exchange Commission has identified measures such as risk assessments, Incident response plans and penetration testing as elements of a robust cybersecurity program for public companies and SEC registrants.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Public companies are required to publicly report material cybersecurity risks, including material past Incidents. Even if a past Incident is not material, companies should consider them in evaluating their disclosures regarding cybersecurity. The SEC has issued guidance regarding the factors public companies should report with respect to cybersecurity. Private companies do not have the same public disclosure obligations, but may need to inform potential investors or purchasers regarding past Incidents or cybersecurity risks.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Yes, many federal and state laws, some of general applicability while some are sector-specific, imposed further requirements on particular organisations. For example, financial institutions are subject to numerous laws and regulations that may overlap with cybersecurity requirements, such as certain duties of oversight that may create obligations with respect to cybersecurity risks created by vendors.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Organisations that publicly announce Incidents involving a large amount of Personal Information will often confront class action litigations filed by plaintiffs whose information was allegedly impacted by the Incident. Typically, these actions involve several theories, including breaches of express or implied contracts, negligence, other common law tort theories, violations of federal or state unfair or deceptive acts or practices statutes or violations of other state and federal statutes.

Contract theories may involve claims of breach of contract where there is a written agreement between the plaintiff and the defendant that contains an express promise of reasonable security measures to protect personal information. Even if such a term is not included in the contract, many plaintiffs will assert a claim of implied contract, arguing that the receipt of a plaintiff's personal information implies a promise to protect the information sufficiently. Tort theories may involve negligence or other common law theories such as invasion of privacy, bailment, misrepresentations with respect to cybersecurity or unjust enrichment. Each of these theories may prove challenging to fit to the data breach context; for example, bailment claims are typically dismissed because plaintiffs cannot allege that they transferred any "property" to the defendant, that the defendant promised to return the "property" or that the defendant wrongfully retained such information.

Consumer protection theories are often alleged, claiming that a victim of a data breach committed unfair or deceptive acts or practices. Deception claims are typically premised on an alleged misrepresentation about the security practices of an organisation. Plaintiffs may also allege that a failure to protect information is "unfair"; although many courts will require a showing of substantial injury or widespread and serious consumer harm. Plaintiffs may also allege violations of other statutes such as the federal Fair Credit Reporting Act or other state laws.

In addition to establishing the elements of their claims, plaintiffs filing in federal court are required to show that they suffered injury-in-fact sufficient to establish standing. Even where an injury alleged is sufficient for standing, it may not be sufficient to state a claim for damages. Some damages theories plaintiffs attempt to assert, with varying success, include risk of future identity theft, credit monitoring costs, other costs related to mitigating risks related to an Incident and overpayment for the products and services associated with the Incident.

While most class actions involve plaintiffs whose information was allegedly compromised, there has been an increase in shareholder derivative and securities fraud actions arising from Incidents as well. In shareholder derivative actions, plaintiffs will typically allege that a company's officers and board of directors breached their fiduciary duties, wasted corporate assets or committed other mismanagement in failing to ensure that the company maintained what the plaintiffs consider appropriate security. As a preliminary step to any derivative action, plaintiffs must first either ask the board of directors to bring the action and, should the board refuse, prove that its refusal was contrary to the board's reasonable business judgment. Alternatively, they must prove that such a request would be futile. Both theories are difficult to prove.

Plaintiffs may also allege securities fraud. To do so, plaintiffs must allege that the company made materially false or misleading statements, typically regarding the state of its cybersecurity posture, and that the company knew about the falsity of such statements.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

As noted, the public announcement of an Incident will frequently result in class actions and other lawsuits being filed against the impacted organisation. Some recent prominent examples include the following:

- Altaba (formerly known as Yahoo!): After announcing an Incident allegedly impacting up to 200 million people, faced consumer class action, shareholder derivative action and securities fraud action, in addition to regulatory investigations, which it ultimately agreed to settle.
- Home Depot: Suffered an Incident related to its payment card terminals. Home Depot settled actions brought by consumers and banks, which alleged that Home Depot had failed to implement adequate security measures. Home Depot also faced a derivative action, which was dismissed. On appeal, the action was settled after Home Depot agreed to adopt certain security procedures.
- Target: Suffered an Incident related to payment card data at its retail stores. Target faced consumer and shareholder actions and also an action brought by banks related to the theft of payment card data.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes, plaintiffs in data breach actions will often accuse the defendant of negligence or other tort law violations. A preliminary question any plaintiff must answer is whether there is any duty to protect the plaintiffs' information. The answer to that question may vary by state. Courts in several states have found no common law duty to protect personal information, while courts in other states have found such a duty under particular facts and circumstances. In *Dittman v. UPMC d/b/a The University of Pittsburgh Medical Center*, for example, the Pennsylvania Supreme Court found that an employer owes a duty to employees to use reasonable care to safeguard what the court described as the employee's "sensitive" personal data when storing it on an internet-accessible computer system.

The California Consumer Privacy Act creates a data breach right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove that the impacted business failed to implement and maintain reasonable and appropriate security practices.

In some states, defendants may assert the economic loss doctrine, which generally provides that contracting parties seeking damages for purely economic losses must seek damages in contract rather than in tort.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Standalone cyber insurance policies typically cover both third-party liabilities arising from the defence and settlement of Incident-related claims, along with first-party cover for the policy holder's own losses, which could include investigation costs, legal fees, notification costs and the costs incurred in providing credit monitoring and identity theft services. Cyber insurance policy forms are typically not standardised and vary significantly from carrier to carrier.

General liability or other policies may, in some instances, cover cyber-related losses, but costs related to Incidents are often excluded.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations specific to cyber insurance, but some states do not allow for insurance against certain violations of law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) Employees generally have broad latitude to monitor employees for cybersecurity purposes, although they generally need to disclose such monitoring to the employee in a written policy. Employers generally are subject to the Wiretap Act, which includes prohibitions related to the interception of electronic communications in transit. Connecticut and Delaware expressly require notice prior to any monitoring of employees.
(b) Generally, employees are not required by law to report an Incident, but almost all companies require such reporting by policy.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Many laws protect whistle-blower reports, such as the Sarbanes-Oxley Act, which is applicable to reports of fraud and securities violations at publicly traded companies. Many employers will include in their policy documents protections for whistle-blowers.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement retains numerous powers to investigate Incidents. In addition to standard warrant and subpoena powers, law enforcement may seek records stored by electronic communication services or remote computing services through the Stored Communications Act, intercept communications in transit through the Wiretap Act or obtain dialling or routing information through the Pen Register statute. The CLOUD Act authorises law enforcement to access certain information held by a United States-based service provider, even if the data is located in another country.

For Incidents involving national security or terrorism, law enforcement may have additional powers. Under the Foreign Intelligence Surveillance Act ("FISA"), the government can obtain information, facilities or technical assistance from a broad range of entities. National Security Letters ("NSLs") offer an additional investigative tool for limited types of entities.

Federal regulatory authorities such as the FTC, SEC and the OCR have powers to investigate Incidents within their respective jurisdictions. State regulators may also investigate Incidents to determine whether any state laws were violated.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under the Communications Assistance for Law Enforcement Act ("CALEA"), law enforcement requires certain telecommunications carriers and manufacturers to build into their systems or services necessary surveillance capabilities to comply with legal requests for information.

No general U.S. laws expressly require organisations to implement backdoors in their IT systems or provide law enforcement authorities with encryption keys. Under the All Writs Act, some courts in some instances have ordered reasonable assistance, including in one notable case, requiring Apple to provide assistance in circumventing security features – which Apple successfully resisted until it was moot.

Edward R. McNicholas is a co-leader of Ropes & Gray's privacy & cybersecurity practice. He represents technologically sophisticated clients facing complex data, privacy and cybersecurity issues. His clients include financial institutions, insurance companies, branded pharma companies, technology communications companies and select retailers. He is lead editor of the PLI Treatise, *Cybersecurity*. Recognised by the National Law Journal as a "Cybersecurity & Data Privacy Trailblazer", Ed has defended companies in dozens of significant data breaches. Mr. McNicholas previously served as an Associate Counsel to President Clinton, where he advised senior White House staff regarding various investigations. Mr. McNicholas received his J.D. from Harvard Law School, where he was an editor of the Harvard Law Review. He received his A.B. from Princeton University and served as a clerk at the U.S. Court of Appeals for the Fourth Circuit.

Ropes & Gray
2099 Pennsylvania Ave, NW.
Washington, DC 20006-6807
USA

Tel: +1 202 508 4779
Email: Edward.McNicholas@RopesGray.com
URL: www.ropesgray.com

Kevin J. Angle is counsel in the Ropes & Gray's privacy & cybersecurity practice. He represents a broad range of companies on privacy and cybersecurity compliance matters, Incident response and transactional diligence. Kevin helps clients to anticipate and address potential areas of legal exposure and to structure privacy programs to minimise potential liability. Kevin graduated from Columbia Law School and was an editor of the Columbia Law Review. After law school, he completed a clerkship for then Judge Carol Bagely Amon of the U.S. District Court for the Eastern District of New York.

Ropes & Gray
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
USA

Tel: +1 617 951 7428
Email: Kevin.Angle@RopesGray.com
URL: www.ropesgray.com

Ropes & Gray is a leader in helping clients navigate the increasingly complex legal landscape surrounding data, including managing complex global advisory matters, responding to litigation and investigations stemming from security Incidents and alleged privacy violations, and advising on transactions involving the acquisition and management of data.

www.ropesgray.com

ROPES & GRAY

Venezuela

LEĜA

Carlos Dominguez

Hildamar Fernandez

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes, according to article 6 of Special Law Against Cybercrime any unauthorised access is considered a legal offence. As this is a criminal offence, anyone who acquires, uses, modifies or removes personal data without consent or have exceeded/misused the consent given, shall be punished with imprisonment ranging from one to five years.

Denial-of-service attacks
Yes, according to article 7 of Special Law Against Cybercrime, anyone who intentionally destroys, damages, modifies or performs any act that alters the operation or disables a system that uses information technologies or any of the components that comprise it, shall be punished with imprisonment ranging from four to eight years and receive a fine of 400 to 800 tax units. Also, anyone who destroys, damages, modifies or disables the data or information contained in any system will incur the same penalty.

The penalty shall be from five to 10 years in prison and a fine of 500 to 1,000 tax units, if the effects indicated in this article are made through the creation, introduction or intentional transmission, by any means, of a virus or similar programme.

For critical infrastructures, the provisions of article 10 apply with an aggravating circumstance due to unauthorised access or sabotage to protected systems. The penalties provided for in the preceding articles shall be increased by one-third to one-half when the events provided for therein or their effects fall on any of the components of a system that uses information technologies protected by security measures, that is intended for public functions or that contains personal or proprietary information of restricted use on persons or groups of natural or legal persons. For critical infrastructures, the provisions of article 10 apply, with an aggravating circumstance due to unauthorised access or sabotage to protected systems. The penalties provided for in the foregoing articles shall be increased by between one-third and one-half when the events provided for therein or their effects fall on any of the components of a system that uses information technologies protected by security measures that is intended for public functions or that contains personal or proprietary information of restricted use on persons or groups of natural or legal persons.

Phishing
In Venezuela, phishing is envisaged as a means of commission to obtain information; however, the criminal offence with which this type of act has been criminalised is through the application of article 10 of the Special Law against Cybercrimes, which punishes anyone who improperly obtains, discloses or disseminates the data or information contained in a system that uses information technology or in any of its components, shall be punished with imprisonment of four to eight years and receive a fine of 400 to 800 tax units. The penalty shall be increased by one-third to one-half if the offence referred to in this article is committed for the purpose of obtaining a benefit for oneself or for another.

The increase shall be from one-half to two-thirds if the security of the State is endangered, the reliability of the operation of the institutions concerned is endangered, or if any damage results for natural or legal persons as a result of the disclosure of information of a confidential nature.

Also, according to article 21 of Special Law Against Cybercrime, any person who through the use of information and communication technologies, capture, intercept, interfere, reproduce, modify, divert or delete any data message or signal of transmission or external communication, will be punished with imprisonment from two to six years and receive a fine of 200 to 600 tax units.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes, see our answer above in section "Denial-of-service attacks".

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
It is a criminal offence according to article 10 of Special Law Against Cybercrime. Anyone in possession or use of hardware, software or any other system shall be punished with imprisonment from three to six years and receive a fine of 300 to 600 tax units.

Similarly, article 19 penalises anyone who, without being duly authorised to issue, manufacture or distribute smart cards or analogous instruments, receives, acquires, possesses, transfers, commercialises, distributes, sells, controls or guards any equipment for the manufacture of smart cards or instruments intended for the same purposes or any equipment or component that captures, records, copies or transmits the data or information from said cards or instruments, shall be punished with imprisonment of three to six years and receive a fine of 300 to 600 tax units.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes, according to article 14 of Special Law Against Cybercrime, anyone who, through the use of information and communication technologies, using any manipulation in systems or any of its components, or in the data or information contained therein, is able

to insert false or fraudulent instructions, which produce a result that allows obtaining an unfair benefit to the detriment of others, will be punished with imprisonment of three to seven years and receive a fine of 300 to 700 tax units.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Yes, according to article 13 of Special Law Against Cybercrime, anyone who through the use of information and communication technologies, access, intercept, interfere, manipulate or use in any way a system or means of communication to seize tangible or intangible assets by subtracting them from their holder, in order to procure an economic benefit for itself or for another, will be punished with imprisonment of two to six years and receive a fine of 200 to 600 tax units.

Also, if the crime was committed by breach of confidence of a current or former employee, it will be qualified as an aggravated offence and the penalty shall be increased by one-third, within its lower and upper limits.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
According to the Special Law Against Cybercrime, all unauthorised access and sabotage offences relating to unauthorised access to systems hacking, computer sabotage and distribution of viruses, computer espionage, computer forgery, and computer fraud will be severely punished.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the Special Law Against Cybercrime establishes in its article 3 that when any of the crimes provided in the Special Law Against Cybercrime are committed outside the territory of Venezuela, the perpetrator shall be subject to the provisions of said law if within the territory of Venezuela there have been effects of the punishable act, and the person responsible has not been prosecuted for the same fact or has evaded judgment or conviction by foreign courts.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The law imposes strict liability.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Yes, cybercrimes are considered transnational organised crime felonies and are similarly typified in the National Security Law which typifies the use of technology for the commission of punishable acts that threaten State security. The most recent case of sabotage to critical infrastructure and terrorism is related to the directors of the interconnection company Credicard.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- Venezuelan Special Law against Cybercrime.
- Communications Privacy Law.
- Organic Code of Criminal Procedure.
- Law of Data Messages and Electronic Signatures.
- Decree No. 825, regarding the Access and Use of the Internet as a Priority Policy for Cultural, Economic, Social and Political Development.
- Decree with Rank Value and Force of Law of Simplification of Administrative Procedures.
- Law of Info government.
- Organic Law on Telecommunications.
- Organic Law for the Protection of Children and Adolescents.
- Law on Banking Sector Institutions.
- Organic Law Against Organized Crime and Financing of Terrorism.
- SUSCERTE's regulation No. 004-10 which encourages the use of Electronic Certificates and Electronic Signatures. Official Gazette No. 39.432 of 05/26/2010.
- SUSCERTE's regulation No. 009-10 Regulation of Classification and Treatment of Information. Official Gazette No. 39.578 of December 21, 2010.
- SUDEBAN's Resolution No. 641.10 regarding the Rules Regulating the Use of Electronic Banking Services. Official Gazette No. 39.597 of January 19, 2011.
- Regulations on Information Technology, Dematerialized Financial Services, Electronic, Virtual and Online Banking for Entities Subject to the Control, Regulation and Supervision of the Superintendency of Banks and Other Financial Institutions.

There is currently no specific data protection law nor a specific regulatory body on Data Protection in Venezuela. In any case, competence has been partially regulated in the Law of Info government, although it has not yet been implemented.

However, the Supreme Court has interpreted that the right to personal data under article 28 of the National Constitution is a fundamental right that allows individuals and entities to control the access and use of their personal data by third parties. Disclosure without their consent, is thus, prohibited. In cases of International transfer of data to territories whose legislation does not guarantee a minimum protection to personal data, it is not permitted.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

Yes, there are cybersecurity requirements under Applicable Laws applicable to critical infrastructure in our jurisdiction. VENCERT

is the National Management System of Telematic Incidents of the Bolivarian Republic of Venezuela and is a team of public and private organisations related to the critical infrastructure of our jurisdiction, tasked with the prevention and management of Incidents. All entities which are a part of VENCERT must abide to its convention.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, but only the organisations in the financial services sector. These organisations are obliged to: (a) establish clauses in the technology services contracts enjoyed with third parties in which enough cybersecurity is guaranteed; (b) establish in their organisational structures an independent area of information security; (c) oblige their employees to sign a confidentiality agreement; (d) generate audit reports; (e) establish mechanisms to prevent the traffic of data in and out of the organisation by unauthorised personal; (f) establish inside their network applications allowing the prevention, detection and elimination of computer viruses; (g) restrict access to programmes that could modify the data in the production environment; and (h) the measures mentioned in question 4.2.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No, it will not.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

All organisations are required to report to the police and judicial authorities all the requested information in case of a penal investigation behind an Incident, as long as there is a court order that requests said report, which will establish the nature and scope of the information requested. Every penal investigation must always be under the order and supervision of the Public Prosecutor of the Public Ministry.

Organisations of the financial services sector are required to make audit reports of Incidents and potential Incidents to the Superintendence of Banks and Financial Institutions (SUDEBAN).

All organisations which are a part of VENCERT are required to report all the information requested of the Incident or potential Incident to VENCERT (see question 2.2 above).

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Yes, the organisations are permitted to voluntarily share information with VENCERT, the Public Ministry and the bodies of investigation specialised in the area (see question 2.2). However, they cannot share private information of the persons involved in the Incident or potential Incident without their consent, especially if that information is related to the health, law and financial services sector.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

VENCERT has the expectation and there is the possibility that the Incident is to be considered a crime, which would trigger the obligation of the organisation to denounce the Incident as a crime. Also, SUDEBAN establishes the obligation in its normative (see question 2.5).

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, they do not.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Public Prosecutor, SUDEBAN and VENCERT.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Criminal investigation and possible coercive measures.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Criminal investigation and possible measures related to prison.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
It is not prohibited but it could configure espionage and that is a crime.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
It could be interpreted as sabotage and it is a crime.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
It is not prohibited by our law.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

There is not a consolidated market practice with respect to information security in our jurisdiction or any common deviations from the strict legal requirements under Applicable laws. However, in the case of Banking, there is a regulation that establishes the mechanisms for its protection.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes, in both sectors there are specific legal requirements in relation to cybersecurity, especially in the financial services sector. In the Telecommunications sector, the organisations have the obligation to use the technical tools and implement the appropriate procedures to prevent Incidents.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

When the Incident takes place: (a) by a decision of the organs of the company; (b) in the area of activity of the company; (c) with resources of the company; or (d) in the exclusive and preferent interest of the company.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Yes, but only the companies in the financial services sector.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

In case of Incidents, the companies have the obligation to provide all the information required by the legal and police authorities.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, they are not.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the event of an Incident, we believe that the following actions may be brought, meaning that the plaintiff may bring, according to the Venezuelan Civil Code, an action before the civil courts on the grounds of:

1. **Damages:** In this case, the plaintiff shall provide proof of the following: (i) the damages caused by the defendant; (ii) the relation between the actions of the defendant and the outcome (damages); (iii) the plaintiff shall request an amount as a compensation; and (iv) the plaintiff will be asked to fulfil the requirements of the specific civil responsibility, as regulated by article 1.185 of the VCC.
2. **Emerging Damage:** In this case, the plaintiff shall provide proof of the following: (i) the effective loss caused by the defendant; (ii) the effective relation between the actions of the defendant and the outcome (the loss); and (iii) the plaintiff shall request and provide proof the amount of the compensation, as regulated by article 1.273 of the VCC.
3. **Loss of profit:** In this case, the plaintiff shall provide proof of the following: (i) the loss of profit caused by the actions of the defendant; (ii) relation between the actions of the defendant and the outcome; (iii) the plaintiff shall request the amount of the compensation; and (iv) if the plaintiff is following the grounds of a specific kind of civil responsibility, the court will request the fulfilment of the responsibility's specific elements, as regulated by article 1.273 of the VCC.
4. **Non-material damage:** The plaintiff will be required to provide proof of the following: (i) the grounds on the non-material damage; (ii) the specific non-material damage; (iii) the moral/non-material impact of the damage on the plaintiff; and (iv) the plaintiff shall request the amount of the compensation, as regulated by article 1.196 of the VCC.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There are no relevant examples to highlight within the Venezuelan jurisdiction.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes, the Special Law Against Cybercrime establishes strict liability towards the offences regulated within it.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

The Law regarding the Insurance Activity does not rule out this possibility in Venezuela, meaning that the organisations could take out insurance on the matter of the Incidents herein named, meanwhile, the regulatory rules that govern the Insurance Contract establish some limits regarding liability exclusions – if there is no agreement between the parties – over the acts of foreign enemies, terrorism, actions made by organisations with the purposes of overthrowing the government, which could include cyber activities such as those specified above.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

The Law of the Insurance Activity does not establish any limitation towards the insurance coverage against any loss; it is the case that the regulatory rules that govern the Insurance Contract establish some limits regarding liability exclusions on acts of foreign enemies, terrorism, actions made by organisations with the purpose of overthrowing the government, which could include cyber activities such as those specified above.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

a) The law establishes some requirements to be met in the financial and telecommunications sector. Regarding the video surveillance and monitoring of work tools it is permitted, but the employee must be notified.

b) No, at the moment our law does not regulate any of the cases indicated above. Given that it is not prohibited, we consider that our law does allow the monitoring of employees, however, we highly recommend prior notification of such activity to the employees. Regarding the obligation of reporting any cyber risks, a clause could be established by contract.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, in our country there are no applicable laws that prohibits or limits the reporting of cyber risks.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In Venezuela, the scientific technical police has wide investigatory powers. However, all the activity related to the investigation must always be under the order and supervision of the Public Prosecutor.

Related to the investigation of Incidents and possible computer crimes, the National System has a National Center for Forensic Informatics and the Division Against Computer Crimes and the Forensic Laboratory of the Corps of Criminal Scientific Investigations and Criminalistics are empowered to do so.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes – they are established in the abovementioned regulations, it is even a contractual requirement in the case of the Banks. Similarly under an investigation, if the company has any of these methods, they are obliged to cooperate by providing them to the body conducting the investigation.

Carlos Dominguez joined LEĜA as an associate in 1996 and became a partner in 2006. He is a member of the Board of Directors and Co-Managing Partner of LEĜA. After he got his law degree, Carlos specialised in civil litigation, and has since extended his career to alternative dispute resolution. He has represented renowned national and international corporations in disputes with international impact, such as breach of contract, corporate disputes, litigation concerning falsification and protection of intellectual property rights in general, debt collection, bankruptcy, product liability, among others. He has held important leadership positions within the International Bar Association and World Services Group.

LEĜA
Av. Eugenio Mendoza.
La Castellana Tower, 7th Floor
Urb. La Castellana
Caracas, 1060
Venezuela

Tel: +58 212 277 2206
Email: cdominguez@lega.law
URL: www.lega.law

Hildamar Fernandez is a criminal lawyer with training in Technology's Land ICT's Law. She has extensive experience in drafting and implementing Security Policies and providing instruction on investigations in the area of Cybercrimes and Telematic Incidents. Hildamar has extensive experience in the areas of Electronic proof practice, Data Protection implementation and use of Electronic Signature, Electronic Government, and Organized Crime. She is an International Lecturer in High Technology Law, Electronic Certification, Computer Security and Cybercrimes.

LEĜA
Av. Eugenio Mendoza.
La Castellana Tower, 7th Floor
Urb. La Castellana
Caracas, 1060
Venezuela

Tel: +58 212 277 2254
Email: hfernandez@lega.law
URL: www.lega.law

LEĜA is a leading law firm in Venezuela enjoying the highest international reputation, with a modern approach to the practise of law supported by the use of technology. With 15 practice areas covering all branches of law and 23 industrial sectors, formed on the experience of our professionals, the firm guarantees a practical and successful approach for each industry. Leĝa is one of the largest and most prestigious law firms in Venezuela, with numerous individual awards by its professionals, and all its areas of practice own the appreciation from the most important legal directories in the world.

Regarding data privacy and protection, we provide counsel on data privacy, bank secrecy, employee engagement and freedom of information and speech. Our team of experts have plenty of experience drafting and reviewing internal policies and contracts with third parties in order to include this kind of protection. We also advice our clients in adopting best practices for data collection and consents, as well as in data transfers and ethics.

As part of our services in this area, we also represent and defend our clients in judicial and/or administrative proceedings as well as in labour and criminal litigation arising from eventual misconducts or violations of these provisions.

www.lega.law

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class and Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media and Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group