Deloitte.

Secure Vigilant Resilient

Transforming cybersecurity in the Financial Services Industry

New approaches for an evolving threat landscape

"2013 has been the noisiest year ever. We are seeing exponential growth in terms of volumes and numbers of attacks. This is not trending down…"

— Anthony Belfiore, head of global cybersecurity, J.P. Morgan[6]

Content

Deloitte named a global leader in Cyber Security Consulting by Kennedy

Source: Kennedy Consulting Research & Advisory; Cyber Security Consulting 2013; Kennedy Consulting Research & Advisory estimates. © 2013 Kennedy Information LLC
Reproduced under license.

Deloitte named a leader in Information Security Services Consulting by Forrester

Source: Forrester Research, Inc., The Forrester Wave™: Information Security Consulting Services Q1 2013, Ed Ferrara and Andrew Rose, February 1, 2013

Deloitte South Africa named Business Continuity Innovation (BCI) Award winners, 2014

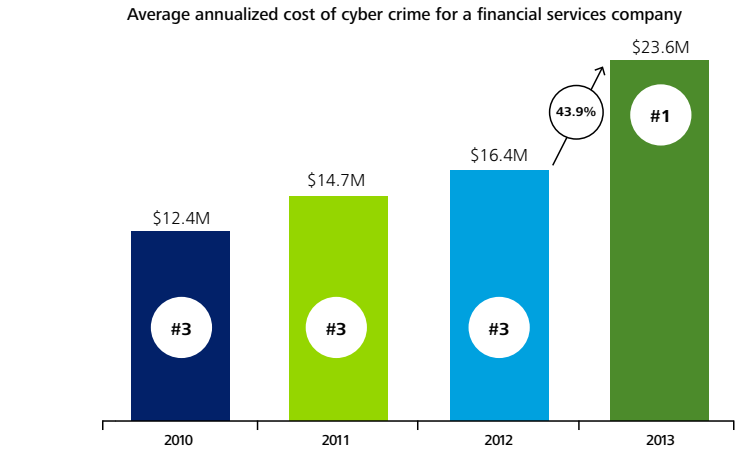
Transforming cybersecurity

Just like Cobb, cybercrime perpetrators begin by identifying their targets' vulnerabilities and gathering intelligence required to breach their systems.

In the recent science fiction film Inception, protagonist Dominic Cobb infiltrated his victim's dreams to gain access to business secrets and confidential data. He would then use this knowledge to influence things in his (or his client's) favour. Cobb's success depended on his ability to manipulate victims through greater understanding of their human vulnerabilities. Just like Cobb, cybercrime perpetrators begin by identifying their targets' vulnerabilities and gathering intelligence required to breach their systems.

Armed with this intelligence, they navigate their targets' complex systems, establish covert presence and often remain undetected for a long time.

Exhibit 1: Many financial services companies are seeing increased costs of cybercrime



(#) – Denotes rank in terms of the average annualized cost of cyber crime to organizations in that industry

Source: Ponemon Institute[1,2] and Deloitte Center for Financial Services analysis

It is clear that the growth in cybercrime has continued, if not accelerated, in the financial services industry (Exhibit 1). US financial services companies lost on average $23.6 million from cybersecurity breaches in 2013[3], which represent the highest average loss across all industries.

To underscore the rapid rise in cyber threats, this number is 43.9% higher than in 2012, when the industry was ranked third, after the defence and utilities & energy industries[4]. While this trend is not to be ignored, these actual losses are sometimes not meaningful to firms' income statements. The potentially greater impact from cybercrime is on customer and investor confidence, reputational risk and regulatory impact that together add up to substantial risks for financial services companies. A recent global survey of corporate C-level executives and board members revealed that cyber risk is now the world's third corporate-risk priority overall in 2013[5]. Interestingly, the same survey from 2011 ranked cybersecurity as only the twelfth-highest priority – a rapid rise explained perhaps in part by the evolving nature of the risks themselves.

In the movie Inception, although Cobb succeeded in conning most of his victims, he faced stiff resistance from Mr Fischer, whose strong automated self-defence mechanisms jeopardised the attackers' plans several times. However, every time Cobb's team faced an obstacle, they persevered, improvised and launched a new attack. Real-life cyber-attacks are, of course, far more complex in many ways than the challenges and responses between Cobb and Fischer. That said, the film does provide an interesting analogy that in many ways illustrates the problems that financial services companies face when dealing with cybercrime.

The interplay between attacker and victim is indeed a cat-and-mouse game in which each side perpetually learns and adapts, leveraging creativity and knowledge of the other's motives to develop new offensive tactics and defensive postures. The relatively static compliance or policy-centric approaches to security found in many financial services companies may be long outdated. The question is whether today's industry can create a dynamic, intelligence-driven approach to cyber risk management not only to prevent, but also detect, respond to and recover from the potential damage that results from these attacks. As such, transformation into a secure, vigilant and resilient cyber model will have to be considered to effectively manage risks and drive innovation in the cyber world.

"Our adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organised criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply or other infrastructure; and hacktivist groups who are trying to make a political or social statement."

— Richard A. McFeely, executive

The evolving cyber-threat landscape

Although cyber attackers are aggressive and likely to relentlessly pursue their objectives, financial services companies are not passive victims. The business and technology innovations that financial services companies are adopting in their quest for growth, innovation and cost optimisation are presenting, in turn, heightened levels of cyber risks. These innovations have likely introduced new vulnerabilities and complexities into the financial services technology ecosystem. For example, the continued adoption of Web, mobile, cloud and social media technologies has likely increased opportunities for attackers. Similarly, the waves of outsourcing, offshoring and third-party contracting, driven by a cost reduction objective, may have further diluted institutional control over IT systems and access points. These trends have resulted in the development of an increasingly boundaryless ecosystem within which financial services companies operate, and thus a much broader "attack surface" for the threat actors to exploit.

Cyber risk is no longer limited to financial crime Complicating the issue further is that cyber threats are fundamentally asymmetrical risks, in the sense that often times, small groups of highly skilled individuals with a wide variety of motivations and goals have the potential to exact disproportionately large amounts of damage.

Yesterday's cyber risk management focus on financial crime was – and still is – essential. However, in discussions with our clients, we hear that they are now targets of not only financial criminals and skilled hackers, but also increasingly of larger, well-organised threat actors, such as hacktivist groups driven by political or social agendas and nation-states, to create systemic havoc in the markets.

An illustrative cyber threat landscape for the banking sector (Exhibit 2) suggests the need for financial services firms to consider a wide range of actors and motives when designing a cyber-risk strategy. This requires a fundamentally new approach to the cyber-risk appetite and the corresponding risk-control environment.

"We went from organised crime, (which are) financially motivated groups who could afford to make an investment, to hacktivists, guys with a social agenda, who are not trying to steal your money."

— Lou Steinberg, chief technology officer, TD Ameritrade[10]

Did you know?

- Financial services companies are most vulnerable to cyber-attacks.
- The financial services industry topped the list of 26 different industries that cyber criminals most targeted.[8]
- Financial services remains the industry most susceptible to malicious email traffickers, as consumers are seven times more likely to be the victim of an attack originating from a spoofed email with a bank brand versus one from any other industry.[9]

Exhibit 2: A diverse array of cyber-attack actors and impacts

A typical cyber-risk heat map for the banking sector

	IMPACTS						
ACTORS	Financial theft/ fraud	Theft of intellectual property on strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life/ safety	Regulatory
Organised criminals	↑↑	→	↓	↓	↑↑	↓	↑↑
Hacktivists	↑	→	↑↑	↑	↑↑	↓	↑
Nation-states	↑	↑	↑↑	↑↑	↑↑	↓	↑↑
Insiders	↑↑	↑	↑	↑	↑	→	↑
Third parties	↑	→	→	→	↑↑	↓	↑↑
Skilled individual hackers	↑↑	↑	↑	↑	↑	↓	↑

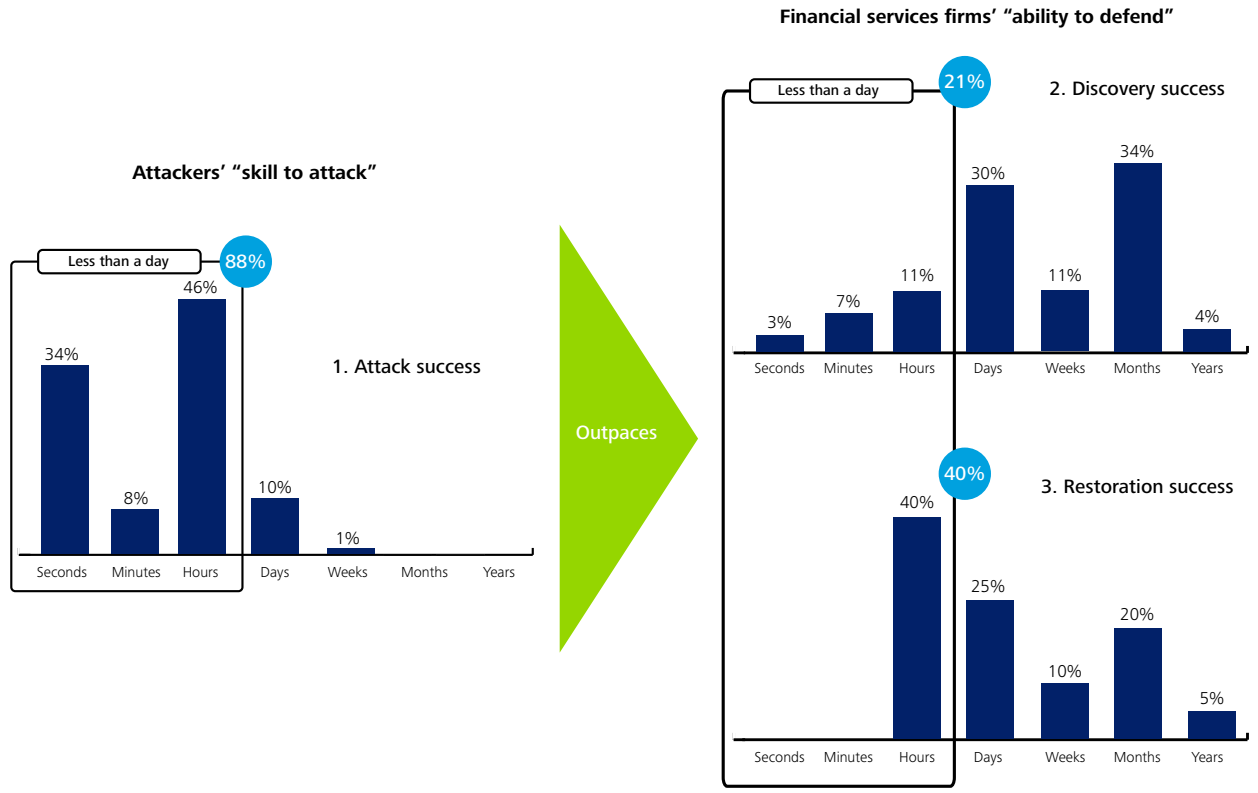
↑↑ Very high ↑ High → Moderate ↓ Low

The speed of attack is increasing while response times are lagging

Threat actors are increasingly deploying a wider array of attack methods to stay one step ahead of financial services firms. For example, criminal gangs and nation-states are combining infiltration techniques in their campaigns, increasingly leveraging malicious insiders. As reported in a Deloitte Touche Tohmatsu Limited (DTTL) survey[11] of global financial services executives, many financial services companies are struggling to achieve a level of cyber-risk maturity required to counter the evolving threats.

Although 75% of global financial services firms believed that their information security programme maturity is at level three or higher[12], only 40% of the respondents were very confident that their organisation's information assets were protected from an external attack; and that is for the larger, relatively more sophisticated financial services companies. For mid-tier and small firms, the situation may be much worse, both because resources are typically scarcer and because attackers may see them as easier targets. In a similar vein, the Snowden incident has perhaps increased attention on insider threats as well.

Exhibit 3: Global financial services firms' response time to attacks indicates significant gaps in preparedness



1. Attack success (time to compromise): Measures time from the first malicious action taken against the victim until the point at which an information asset is negatively affected.
2. Discovery success (time from compromise to discovery): Measures time from initial compromise to when the victim first learns of the incident.
3. Restoration success (time from discovery to containment): Measures time between the discovery of a breach to when it is successfully contained.

Percent might not add up to 100 due to rounding errors.

Source: Verizon Risk[13] and Deloitte Center for Financial Services analysis

These inadequacies become more apparent when we look at the data. As shown in Exhibit 3, the Deloitte Center for Financial Services has analysed data from an annual investigative report on data security by Verizon and found that in 2013, 88% of the attacks initiated against financial services companies are successful in less than a day. However, only 21% of these are discovered within a day; and even worse, in the post-discovery period, only 40% of them are restored within that one-day timeframe[14]. The speed of attack, significant lag in discovery rates, and longer restoration time highlight the challenges that financial services firms can face in both detection and response capabilities.

Multipronged approach

A multipronged approach can supplement traditional technologies that may now be inadequate

From the previous analysis, one might be tempted to assume that if 88% of attacks are successful in less than a day, the solution may be found in increased investment in tools and technologies to prevent these attacks from being successful. However, the lack of threat awareness and response suggests that more preventative technologies are, alone, likely to be inadequate. Rather, financial services companies can consider adopting a multipronged approach that incorporates a more comprehensive programme of cyber defence and response measures to deal with the wider array of cyber threats and risks.

The imperative to be secure, vigilant and resilient

Financial services firms have traditionally focused their investments on becoming secure. However, this approach is no longer adequate in the face of the rapidly changing threat landscape. Put simply, financial services companies should consider building cyber risk management programmes to achieve three essential capabilities, namely the ability to be secure, vigilant and resilient (Exhibit 4).

Enhancing security through a "defence-in-depth" strategy

A good understanding of known threats and controls, industry standards and regulations can guide financial services firms to secure their systems through the design and implementation of preventative, risk-intelligent controls. Based on leading practices, financial services firms can build a "defence-in-depth" approach to address known and emerging threats. This involves a number of mutually reinforcing security layers both to provide redundancy and potentially slow down the progression of attacks in progress, if not prevent them.

Did you know?

- Financial services firms will need the highest increase in security spending to avert cyber-attacks
- Financial services companies would face the steepest increase in spending to reach an ideal state of protection – 13-fold rise to $292.4 million per company to fend off 95% of cyber-attacks[15].

"In today's environment, it is unrealistic to expect that defences can prevent all cyber incidents. The financial industry should continue developing capabilities for detecting incidents when they occur, minimising the impact on business and critical infrastructure, and tying these capabilities together in a comprehensive framework. Quantum Dawn 2[16] helped participants understand the need not just to be secure, but also to be vigilant and resilient in the face of cyber threats."

— Ed Powers, national managing partner, cyber risk services, Deloitte & Touche LLP[17]

Enhancing vigilance through effective early detection and signalling systems

Early detection, through the enhancement of programmes to detect both the emerging threats and the attacker's moves, can be an essential step towards containing and mitigating losses. Incident detection that incorporates sophisticated, adaptive, signalling and reporting systems can automate the correlation and analysis of large amounts of IT and business data, as well as various threat indicators, on an enterprise-wide basis. Financial services companies' monitoring systems should work 24/7, with adequate support for efficient incident handling and remediation processes.

Enhancing resilience through simulated testing and crisis management processes

Resilience may be more critical as destructive attack capabilities gain steam. Financial services firms have traditionally planned for resilience against physical attacks and natural disasters; cyber resilience can be treated in much the same way. Financial services companies should consider their overall cyber resilience capabilities across several dimensions. First, systems and processes can be designed and tested to withstand stresses for extended periods. This can include assessing critical online applications for their level of dependencies on the cyber ecosystem to determine vulnerabilities. Second, financial services firms can implement good playbooks to help triage attacks and rapidly restore operations with minimal service disruption. Finally, robust crisis management processes can be built with participation from various functions, including business, IT, communications, public affairs and other areas within the organisation.

Exhibit 4: Improving cybersecurity with a "secure, vigilant and resilient" strategy

Traditionally, the focus has been on being secure. However, the evolving cyber threat landscape may necessitate a shift to a more dynamic approach and well-rounded cybersecurity capability.

Secure: Enhance risk prioritized controls to protect against known and emerging threats, comply with industry cybersecurity standards and regulations.

Vigilant: Detect violations and anomalies through better situational awareness across the environment.

Resilient: Establish the ability to quickly return to normal operations and repair damage to the business.

Source: Deloitte Center for Financial Services analysis

Transforming to a secure, vigilant and resilient model

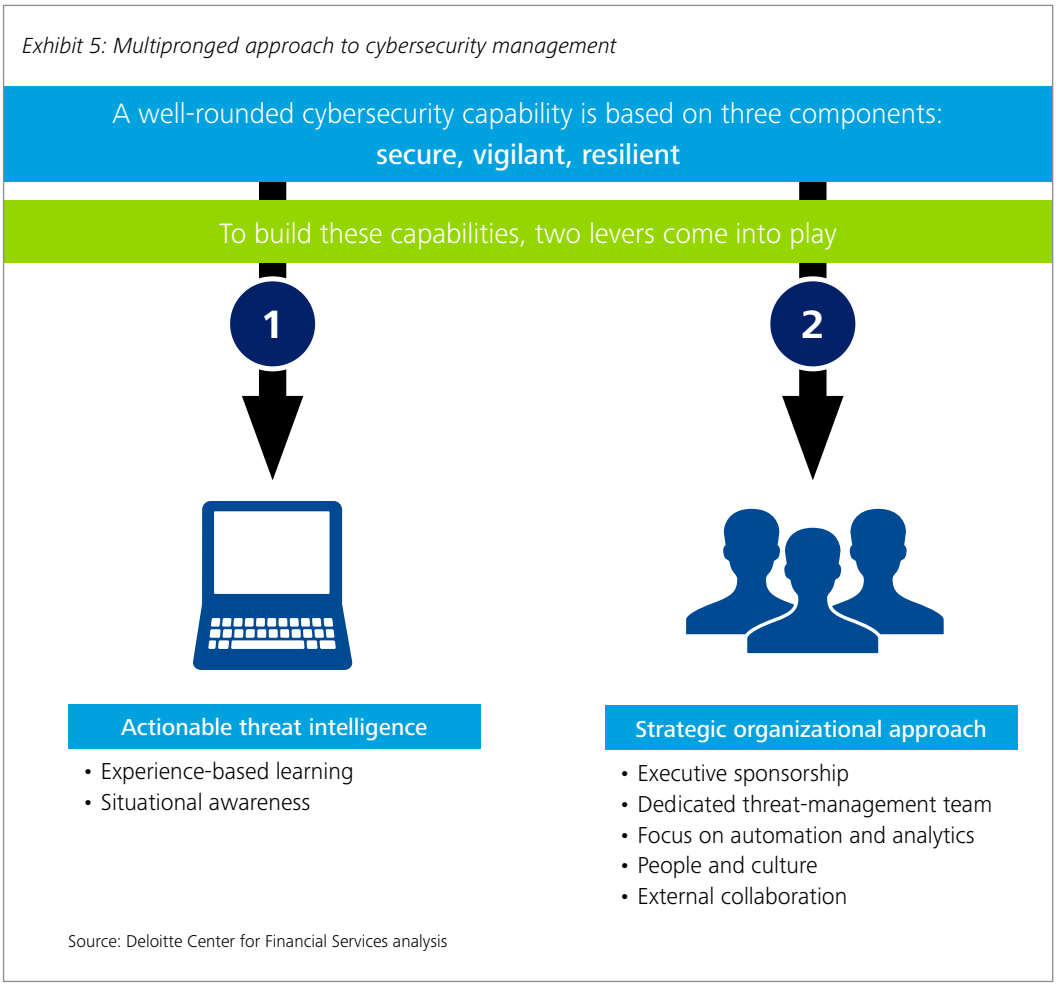
How can financial services firms begin the journey towards establishing programmes to really be more secure, vigilant and resilient and hence transform their cyber risk management programmes? Two important levers can come into play for many financial services companies as they seek to manage evolving cyber threats in the long run (Exhibit 5):

1. Develop actionable threat intelligence in support of a well-rounded capability across all three components of the model.
2. Address the organisational challenges with decisive actions that recognise cybersecurity as a strategic business problem, not just an "IT problem".

Actionable threat intelligence

Financial services executives recognise that becoming a learning organisation where intelligence drives actions is likely to be increasingly important for success across multiple dimensions. The realm of cybersecurity is no different, as real-time threat intelligence can play a crucial role in enabling security, vigilance and resilience. By intelligence, of course, we mean not only the collection of raw data about known threat indicators, as is provided by many vendors in the form of threat-intelligence feeds. Threat intelligence is also the derivation of meaningful insights about adversaries from a wide range of sources, both internal and external, through automated means and through direct human involvement.

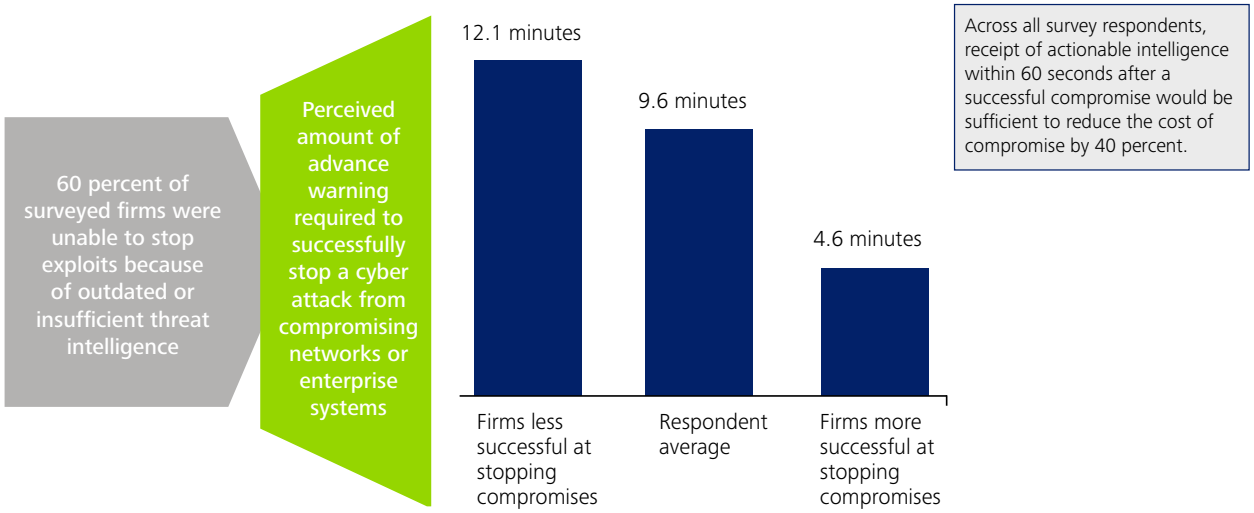
Exhibit 5: Multipronged approach to cybersecurity management



Source: Deloitte Center for Financial Services analysis

Availability of real-time intelligence can help organisations to prevent and contain the impact of cyber attacks. A recent study from the Ponemon Institute revealed that surveyed IT executives believed that less than 10 minutes of advance notification of a security breach would be sufficient time for them to disable the threat[18]. Even with only 60 seconds notification after the compromise, costs of security breaches may be reduced by an average of 40%[19] (Exhibit 6).

Exhibit 6: Opportunity to prevent and contain attacks under various scenarios



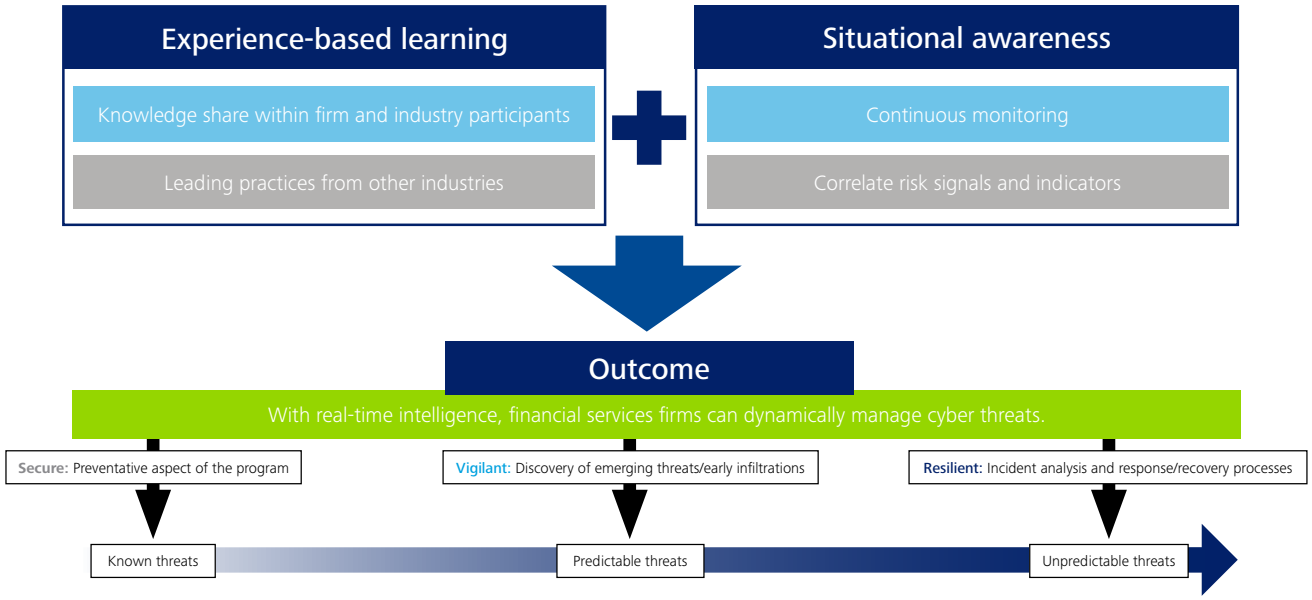
Source: Ponemon Institute[20] and Deloitte Center for Financial Services analysis

To be actionable, threat data should be viewed in a context that is meaningful to the organisation. As a financial services firm develops greater maturity in its data gathering and processing capabilities, automation can be leveraged to better filter and highlight information that is directly relevant to important risk areas. In this way, threat intelligence becomes the foundation on which a firm builds its secure, vigilant and resilient capabilities (Exhibit 7). So, how can financial services companies create that dynamism and move to an intelligence-driven cybersecurity model?

Experience-based learning: Just as cyber attackers play on their target's weak spots, so can financial services firms develop a sound understanding of the attackers and identify their Achilles' heels. Financial services companies can attempt to learn from past intrusions within both the individual firm and at the industry level. Many financial services companies can also borrow lessons from other industries, like aerospace and defence, to implement new techniques, playbooks and controls. These lessons include understanding the nature of the attack, tactics and patterns, and containment strategies, and pose some questions that financial services firms should consider to safeguard themselves from the onslaught of cyber-attacks:

- Who are these attackers and what are their motives?
- How do these cyber attackers manage such high attack success rates?
- Is it just the attackers' expertise, or are the victims unwitting enablers? If yes, in what way can that be fixed?
- What are some of the common challenges that attackers face while infiltrating financial services companies' systems?
- How are other financial services companies/ industries dealing with such attacks?

Exhibit 7: Real-time threat intelligence is the foundation for the new cybersecurity model



Source: Deloitte Center for Financial Services analysis

Situational awareness: Financial services firms can consider supplementing experience-based learning with a continuous monitoring programme, focused on both external and internal threats. Continuous monitoring can help capture the risk signals and indicators across the ecosystem in order to develop a situational awareness of the threat environment. It assists organisations in identifying attack patterns and moving from being reactive to proactive in their defence and response mechanisms. Continuous monitoring also begins to address the speed-of-response issue that attackers are exploiting against the financial services industry.

For many firms, becoming a learning organisation implies a need to develop an approach to address weaknesses in understanding their attackers' motives and methods. Learning from each experience and sharing information both within and outside the organisation will likely help many financial services companies address weaknesses in their ability to discover and recover from attacks.

Did you know?

- Study reveals that IT systems are not employed adequately, if at all, for insider threat detection and response
- Only 6% of the cases of insider fraud (cyber-based) within financial services companies were detected using software and systems.[21]

An ‘IT problem’ becomes a strategic business problem

Though financial services firms may acknowledge the magnitude of the problem that cyber risks pose (not just to them but also to the systemic stability of the market), this imperative is not always adequately recognised or accounted for across the enterprise. A deeper analysis of the successes and failures of cyber threat programmes may suggest some of the following potential actions that leaders can take to develop a more comprehensive organisational approach to cyber risk management:

1	Cyber risk strategy to be driven at the executive level as an integral part of the core company strategy
2	A dedicated cyber threat management team to be established for a dynamic, intelligence-driven approach to security
3	A focused effort to be placed on automation and analytics to create internal and external risk transparency
4	The ‘people’ link in the defence chain can be strengthened as part of a cyber-risk-aware culture
5	Cybersecurity collaboration to be extended beyond company walls to address common enemies

Did you know?
The Financial Services Sector Coordinating Council discusses an agile and risk-based approach

Any cybersecurity framework must be highly structured, yet nimble and flexible enough to adapt in real-time as threats emerge. Standards or guidelines that amount to a static set of “checklists” without an initial risk-based approach may result in institutions being “compliant” without being effectively secure.[22]

Action 1: Cyber risk strategy to be executive-driven with clear accountability

Many of the discussions happening at financial services firms with whom we speak are about cyber risk management accountability models and roles of the business, chief information officer (CIO), chief information security officer (CISO) and IT risk officers. Often, we find that the CISO or IT risk officers are valiantly fighting the cyber battle, with limited support from the executive management team or the broader IT team. We also find that the CISO often struggles in defining his or her role within the context of the lines of defence: “Am I a policy or standards bearer, an operator or an oversight function?” The net result is that these internal struggles can contribute to ineffective cyber risk management programmes.

Potential resolution

If cyber risk is so closely tied to the growth and innovation agenda, why is cyber risk management responsibility often delegated multiple levels down within the organisation? While the CISO or IT risk officer clearly has a very significant role to play, for sustainable success firms may consider appointing a chief operating officer (COO) or chief administrative officer (CAO) equivalent to lead a cross-functional team to drive the cyber risk agenda. By appointing a senior leader and establishing a cross-functional council, firm leadership can send a clear message that cyber risk is an enterprise agenda item and not just a technology issue. The council can take a lead in establishing the risk appetite and can create the cyber risk management strategy for the firm. The council can also precisely define the line-of-defence model for cyber risk management and hold employees accountable. CIOs and their direct reports should consider taking ownership for risk management related both to infrastructure and applications, while human resources and other functions need to understand their roles, particularly in dealing with insider threats. Finally, business leaders can be held accountable for their responsibilities related to data classification and protection.

Action 2: A dedicated cyber threat management unit could be established to launch and sustain a dynamic, intelligence-driven approach to security

We have found multiple scenarios that can lead to ineffective threat management practices. In some – but nowadays rare – cases, many companies don't have a dedicated threat management team. Second, where a team might exist, we often find that the mission is not clear or the team is not adequately resourced to achieve that mission. Finally, we also have found situations where a team is formalised, but the operating model and information flow with the broader IT and business organisation have not been defined.

Potential resolution

Rapid information sharing, active collaboration and collective learning can be critical to the team's ability to reduce detection times and, in many cases, avoid incidents completely. Even if only starting small and with a narrow mission, financial services firms should consider creating a dedicated cyber threat intelligence unit with the responsibility to provide updates to the broader team on threats and controls that require enhancement. This team should have a defined operating model and information flow with other responsible parts of the organisation, including infrastructure, application development, vulnerability management, security operations, incident response and forensics, fraud, etc. This interaction model, supported by applicable processes and tools, may be critical to creating the fabric to be secure and vigilant in cyber space.

Action 3: A focused effort to be placed on automation and analytics to create internal and external risk transparency

Many financial services companies have complex, non-standardised infrastructures and siloed support models that act as major barriers to the desired goals of transparency and rapid information flow. In many companies, foundational capabilities (like good asset and configuration management practices) are often missing or not mature enough. Others do not have transparency into the network traffic flows into and out of their environment; or if they do, they only use it for operational purposes and not for risk management. With recent focus on insider threats, we often find that companies do not have good processes around defining and monitoring sensitive positions, with the result that red flags can be missed.

Potential resolution

Financial services firms should consider revisiting their IT security investments and prioritising investments to create the required automation and analytics in their environment. Unfortunately, this very often can cover a significant number of areas like applications, infrastructure (network and hosts), users, accounts and transactions, to name a few. While this may seem overwhelming, the 80/20 rule applies, and taking an intelligence-driven approach may be useful to help prioritise areas of focus. Financial services companies should also consider storing as much as three to six months' worth of important data for historical analysis purposes. In many large organisations, this amounts to hundreds of terabytes of data, but this is the new reality and the cost of doing business in the cyber world. Social media analytics is another area that many are paying closer attention to for intelligence, brand protection and, perhaps most importantly, during crisis management.

Did you know?
Study reveals inadequate IT security funding in financial services
44% of global financial services firms cite lack of sufficient funding as the primary barrier to implementing an effective IT security programme[23].

Action 4: The 'people' link in the defence chain can be strengthened as part of a cyber-risk-aware culture

The increased frequency of cyber-attacks that focus on people as the "weak link in the chain" has not yet translated into increased investments to address this weakness, nor to creating an overall cyber-aware culture. As an example, spear phishing[24] tests conducted by Deloitte cyber risk services have shown that senior executives and their assistants are often common targets of such malicious attacks. While there are mandatory cyber trainings at several financial services firms, employees often perceive them as theoretical and, hence, boring[25]. Our experience also indicates that in the mid-to-long term, a cyber-aware organisation is likely to have a meaningful return on investment, with cyber-aware employees playing meaningful roles in prevention and detection of attacks and frauds.

Potential resolution

It can be important for financial services companies to understand that employees might possess functional expertise, but do not necessarily have the skills to spot suspicious cyber activities. A significant change in tactics related to cyber training and awareness is likely to be required, with organisations adopting a more "human-centric" approach, which considers user experience and is informative at the same time. Examples of leading practices include cyber war-gaming exercises that bring together different parts of the organisation in real-life simulations, as well as insightful training videos, or perhaps even tablet-based applications for their executives.

"Chasing the latest tools is part of managing cyber risks, but it may not be sufficient; we must truly change the hearts and minds of users on this issue. CIOs should consider focusing more effort on people than technology. And that doesn't mean asking users to click on a 22-page legal agreement that certifies their understanding of corporate security policy. Rather, we should try to use brevity, humour and other modes of engagement to help users understand the organisation's security and privacy challenges and their role in meeting them."

— Larry Quinlan, CIO, Deloitte Services LP[26]

Action 5: Cybersecurity collaboration to be extended beyond company walls to address common enemies

Cyber risk challenges frequently cannot be solved solely within the boundaries of the financial services firm. However, some firms do not spend the time or money to build relationships with other members of their cyber ecosystem. Despite many formal channels of information sharing, real meaningful intelligence is still often shared among trusted peers only. Having points of contact established can help to both prevent and respond to incidents. This need is particularly acute when disaster strikes and financial services companies need support from the ecosystem for crisis-management activities that can often be outside the firm's direct control.

Potential resolution

Financial services companies could greatly benefit from building industry relationships and furthering the public–private partnership. It takes time and effort, but it may pay off in the long run. To prepare for and potentially assist during a cyber-crisis, it is advisable for financial services companies to build relationships with their law enforcement contacts, forensic and incident-response specialists, cyber-savvy law firms, and communications and public relations firms. Financial services firms should also consider building relationships with critical service providers like telecom companies and major hardware and software providers, in turn gaining access to critical resources for emergency needs. Finally, financial services companies can leverage industry associations and government agencies (e.g. the Financial Services Information Sharing and Analysis Centre and the Department of Homeland Security, among others) to further their cause and learn leading practices.

"Quantum Dawn 2 proved that information sharing between the private sector and the government is one of the most effective ways to combat cybercrime… Legislation that promotes this sharing and other activities will help our country more effectively mitigate cyber threats on the financial system."

— Judd Gregg, CEO, SIFMA[27]

Summary

Cyber-attacks on financial services companies are increasingly diverse – and therefore unpredictable – and are here to stay. Many of these continue to be driven, as we know, by financial gain. However, the ranks of attackers have increasingly grown to include others with social or political agendas that seek to destroy systems or create market havoc. At the same time, the current economic climate drives financial services firms continually to create competitive advantage and drive profitability by leveraging new technologies and business methods. The resulting changes can introduce new vulnerabilities that hackers can and do exploit with unrelenting agility.

Inception highlighted how both the attackers and the victims played to their strengths and the other person's weakness. When the attack severity increases, it may likely be a resilient and flexible cybersecurity model that can prepare financial services companies to survive the inevitable cyber risks. As such, financial services firms should consider raising their level of preparedness and evolve into a new cyber risk management paradigm that strives to achieve three fundamental qualities:

Secure

Vigilant

Resilient

- Being **secure** against known threats through risk- driven investment in foundational, preventive controls and policies
- Being **vigilant** by improving the ability to detect emerging threats and anomalous patterns amidst the highly complex and data-saturated environment
- Being **resilient** to enable the organisation to recover from attacks as quickly as possible and minimise both direct and indirect damages

Actionable threat intelligence derived from a wide range of sources and well-defined governance processes, which instil cyber risk awareness, accountability and effective continuous adaptation, can be critical fuel in driving this paradigm shift. For many firms, what are now typically called IT risk management programmes can evolve into executive-driven cyber risk management programmes that are an integral part of strategic business planning. The imperative to transform is a strategic business issue; the financial services companies that master this new approach could likely be at the forefront of the industry because, by incorporating a more agile cyber risk management approach, they may be able to more effectively harness the ongoing digital revolution to their advantage.

Endnotes

1 “2013 Cost of Cybercrime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2013; “2012 Cost of Cybercrime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2012.

2 The study examines the total costs firms incur when responding to cybercrime incidents and include internal security-related activities (detection, investigation & escalation, recovery, ex-post response, containment) and external consequences/costs (information loss or theft, business disruption, equipment damage, revenue loss).

3 “2013 Cost of Cybercrime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2013. 4 “2012 Cost of Cybercrime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2012. 5 “Risk Index 2013,” Lloyd’s, July 2013.

6 Ivy Schmerken, “Cybercrime on Wall Street,” Wall Street & Technology, July 16, 2013.

7 Statement before the Senate Appropriations Committee, Washington, D.C., June 12, 2013.

8 “Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry,” Mandiant, September 23, 2013.

9 “Agari Email Trust Index: 3rd Quarter Edition,” Agari, November 2013.

10 Ivy Schmerken, “Cybercrime on Wall Street,” Wall Street & Technology, July 16, 2013.

11 “2012 DTTL Global Financial Services Industry Security Study,” Deloitte Global Services Limited, September 2012.

12 Survey defines 1-5 levels of maturity of organization’s information security program. Level 3 – defined (set of defined and documented standard processes, some degree of improvement over time); level 4 – managed (process metrics, effective management control, adaption without loss of quality); level 5 – optimizing (focus on continuous improvement, innovation).

13 Subset of data used for “Threat Landscape: Financial Services (Verizon DBIR 2011-2013),” Verizon, September 2013.

14 Ibid.

15 Eric Engleman and Chris Strohm, “Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps,” Bloomberg, January 31, 2012.

16 Quantum Dawn 2 cyber exercise (QD2), hosted by SIFMA on July 18, 2013, enabled over 500 participants from over 50 different entities across the financial sector to run through their cyber crisis response plans including how they would coordinate with the financial sector as a whole and with government agencies to share information.

17 “SIFMA Announces Key Findings of Quantum Dawn 2,” SIFMA, October 21, 2013.

18 “Live Threat Intelligence Impact Report 2013,” Ponemon Institute (sponsored by Norse Corporation), July 2013.

19 Ibid.

20 Ibid.

21 Adam Cummings, Todd Lewellen, David McIntire, Andrew P. Moore, and Randall Trzeciak, “Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,” CERT Insider Threat Center of Carnegie Mellon University’s Software Engineering Institute, July 2012.

22 “Developing a Framework to Improve Infrastructure Cybersecurity,” Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, April 8, 2013.

23 “2012 DTTL Global Financial Services Industry Security Study,” Deloitte Global Services Limited, September 2012.

24 Spear-phishing involves a targeted attack against a specific individual (or related group of individuals) within an organization or professional group that the perpetrator wishes to compromise. It relies on the perpetrator establishing a degree of purported familiarity with the target.

25 “Cyber Training 3.0: New Solutions Addressing Escalating Security Risks,” NASCIO, June 3, 2013.

26 “An Interview with Deloitte Services LP CIO Larry Quinlan,” The Wall Street Journal’s CIO Journal, February 5, 2013.

27 “SIFMA Announces Key Findings of Quantum Dawn 2,” SIFMA, October 21, 2013.

Contacts

South Africa

Dave Kennedy
Managing Director, Risk Advisory, Africa
Tel: +27 11 806 5340
Email: dkennedy@deloitte.co.za

Akiva Ehrlich
Leader: Risk Advisory, Financial Services Industry
Tel: +27 11 806 6175
Email: akehrlich@deloitte.co.za

Cathy Gibson
Africa Leader: Risk Advisory, Cyber Risk & Resilience
Tel: +27 11 806 5386
Email: cgibson@deloitte.co.za

Graham Dawes
Leader: Risk Advisory, Rest of Africa
Tel: +254(0)719892209
Email: gdawes@deloitte.co.za

Danita de Swardt
Director: Risk Advisory
(Johannesburg)
Tel: +27 11 806 5208
Email: ddeswardt@deloitte.co.za

Ashraf van Graan
Associate Director: Risk Advisory
(Cape Town)
Tel: +27 21 427 5711
Email: avangraan@deloitte.co.za

Paul Orffer
Senior Manager: Risk Advisory
(Johannesburg)
Tel: +27 11 806 5567
Email: porffer@deloitte.co.za

Henry Peens
Senior Manager: Risk Advisory
(Johannesburg)
Tel: +27 11 806 5625
Email: hpeens@deloitte.co.za

Designed and produced by Creative Solutions at Deloitte, Johannesburg. (808854/lie)

The Center wishes to thank the following Deloitte professionals for their support and contribution to the report:

- Michelle Chodosh, Marketing Manager, Deloitte Services LP Lauren Fischer, Lead Marketing Specialist, Deloitte Services LP Mary Galligan, Director, Deloitte & Touche LLP
- Lisa DeGreif Lauterbach, Marketing Leader, Deloitte Center for Financial Services, Deloitte Services LP Jennifer O'Neill, Director, Deloitte Services LP
- Ash Raghavan, Principal, Deloitte & Touche LLP
- Beth Ruck, Marketing Leader, Vigilant by Deloitte, Deloitte & Touche LLP Irfan Saif, Principal, Deloitte & Touche LLP
- Surabhi Sheth, Executive Manager, Deloitte SVCS India Pvt Ltd
- Val Srinivas, Research Leader, Banking & Securities, Deloitte Services LP Prasad Yadav, Senior Analyst, Deloitte SVCS India Pvt Ltd