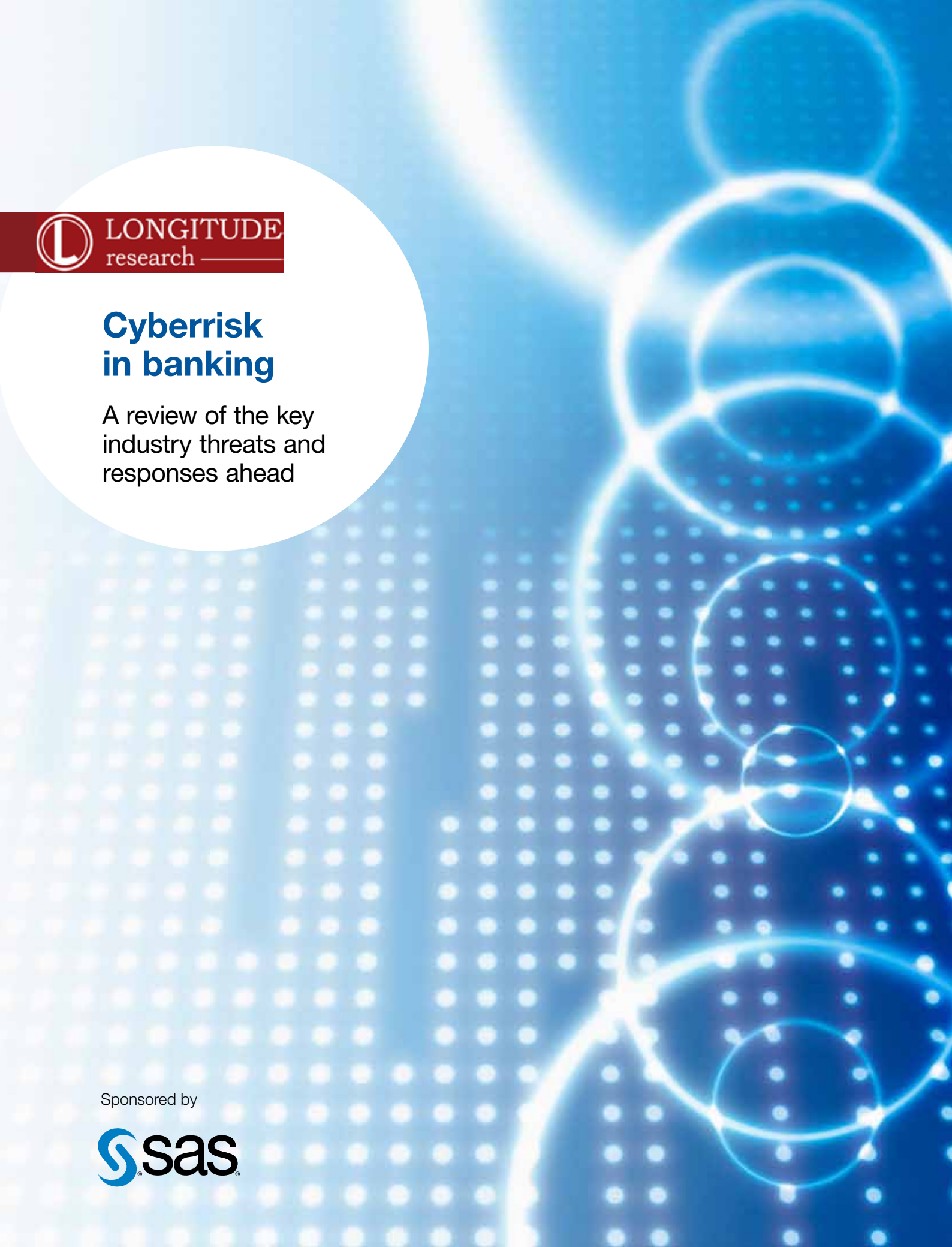

LONGITUDE research

Cyberrisk in banking

A review of the key industry threats and responses ahead

Sponsored by

sas

Table of Contents

Foreword

Cybersecurity is a complex and multifaceted challenge that is growing in importance. It is an issue that not only affects the banks and government agencies that are frequently highlighted through the press; its implications continue to expand beyond that. To counter new and emerging threats, organizations will need to learn from previous threats across a range of industries to proactively meet the challenges ahead.

Most organizations have traditionally viewed cybersecurity as an information technology (IT) problem. Today we know that it must be treated as a broader risk management issue, proliferating the risk-based decision making of such events.

In this effort, we recognize the importance of using data to identify trends and patterns. But there is a lot of data: external threat information, internal and external usage logs, customer information, transaction data and more. Added to this is the increasing challenge of mining the data for useful information in the time frames required as the threats become more sophisticated. Harnessing the big data assets in a proactive manner across the fraud and cybersecurity domains will help combat the ever-changing nature of attacks.

Though cybersecurity is clearly a cross-industry issue, financial institutions are leading a trend towards convergence of fraud and cybercrime prevention technology and operations in support of a holistic approach to cybersecurity. This strategy will require new capabilities, not least to fill gaps in the technology marketplace as part of solving the biggest data challenges to date, and in proactively using better analytics to make real-time, risk-based decisions.

Stu Bradley
Senior Director of SAS Security Intelligence Solutions
September 2013

About the research

The quantitative findings presented in this report come from a survey of 250 respondents in financial services, with 55 percent in retail banking and 45 percent in commercial banking, conducted by Longitude Research. All respondents have influence on, or knowledge relating to, their organization's cybersecurity risks and responses.

Across the sample, one in three respondents is a C-level executive. They are primarily based in the Western Hemisphere, including North America (40 percent), Europe (21 percent) and Latin America (20 percent). Respondents represent a wide range of functions, led by IT (42 percent), finance (21 percent), general management (14 percent) and risk (14 percent). Half work for companies with global annual revenue exceeding US$500 million.

To supplement the quantitative survey results, Longitude Research conducted in-depth interviews with senior executives and experts. They include:

- Richard Frank, International Cybercrime Research Centre, Simon Fraser University
- Brian Lapidus, Senior Vice President and Practice Leader, Kroll Advisory Solutions
- Adel Melek, Managing Director, Global Enterprise Risk Services, Deloitte Touche Tohmatsu Limited
- David Pollino, Senior Vice President and Enterprise Fraud Prevention Officer, Bank of the West
- Poul Otto Schousboe, Head of Group IT Security, Danske Bank
- Chris Smith, Director, Service Engagement and Federal Enterprise Architecture, SAS
- Mike Usher, Director of Information Risk, Prudential Corporation Asia

Executive summary

The rise of the information society has provided a wealth of opportunities for organizations to enhance services to customers through new channels. These have helped to save time, money and effort from an operational perspective. But on the opposite end, cybercriminals are finding new ways to exploit weaknesses and working to develop ever more sophisticated methods of attack – or finding high-tech reinventions of old tricks. The cost to consumers – and to society as a whole – is growing, while a lack of international cooperation allows the trend to continue.

Many of these threats are basic. Simple spam or phishing emails, which encourage users to share information about themselves, continue to be a major problem across industries. But the threat landscape is also becoming increasingly complex. There is a convergence of offline fraud and online crimes, especially in financial services institutions – consider the recent attacks in which international hackers steal data that is then used by local criminals to fraudulently withdraw money at banks. Cybercriminals also look for the weakest links in the information supply chain, which means institutions can come under indirect attack even when their own systems are secure. Third-party providers and other actors hold massive amounts of data about consumers, making them targets as well.

Though cybercrime transcends industry borders, financial institutions often lead the way by experiencing new threats and enhancing their cybersecurity defenses. Based on a survey of 250 banking executives, along with in-depth expert interviews, this report looks at cybersecurity challenges and opportunities specifically as they relate to banks. Among the key findings are:

- **Both technologies and threats are evolving.** Leveraging new channels of communication are important to better serve customers, but keeping pace with emerging technologies—and their associated threats—are also key challenges. Mobile devices and applications are primary examples of the balance between greater efficiency and new kinds of cyberrisks. Some financial institutions struggle in this area, while others find ways to combine usability and security. According to this report's risk radar (see page 7 for details), which is based on our survey findings, phishing, botnets and mobile malware were rated among the most likely threats faced, and also among the ones with the biggest impact.
- **Awareness remains low.** Improved knowledge of threats is often cited as critical to enhance cybersecurity. Banks are trying to educate their customers, in part through new channels of communication such as Twitter and YouTube, in addition to more frequent website updates. Nearly one in three (30 percent) of those polled rate limited customer awareness as a key challenge, making it one of the top four issues faced. But the problem is not solely external: careless employees are often cited as a particular concern, for example. And lack of knowledge sometimes reaches right to the very top of organizations: Nearly one in ten respondents (eight percent) cited a lack of C-suite understanding of the issue as a key challenge.

- **Preparedness for cyberrisks remains patchy.** Just one in five of the executives polled for this study regards their organization's overall preparedness for cybersecurity risks as "high." When reviewed in greater detail, the technology-related aspects of their preparedness perform best, yet only about half of respondents rate their banks as highly prepared. In other key factors, such as internal and external cooperation, and broader legal support, preparedness is even weaker. Most strikingly, less than one in four banks believe their internal resources are highly prepared - perhaps the easiest aspect of preparedness to resolve. But this reflects the fact that banks are currently only willing to spend just enough to ensure customers remain trusting. As such, there appears to be a disconnect between the availability of resources and information and the urge to use them in combating cybercrime.
- **Trust trumps financial losses.** Despite rising losses and the perception that they will continue to increase, banks are only spending just enough on cybersecurity to make customers trust them. Indeed, when asked how significant the impact of cybersecurity attacks has been, nearly twice as many executives pointed to customer trust than those who cited financial losses (39 percent versus 23 percent, respectively). Indicative of this, a majority of banks say budgets rise in line with perceived threats, while a lack of internal resources is cited as one of the key hurdles on the path toward better cybersecurity.
- **A lack of cooperation is hindering progress.** Because many banks are typically only financially liable when their own systems are compromised, there is little incentive for them to cooperate with other stakeholders when it comes to cybersecurity. Although there are exceptions, many financial institutions operate in silos – or only work with each other through industry associations – while expecting others, primarily governments, to deal more effectively with deterring cybercriminals. Overall, just 32 percent of executives describe their firms as "highly prepared" when it comes to external cooperation – and a striking 78 percent say they do not rely on any other parties in dealing with cybersecurity. The problem is particularly acute at the international level as there is a lack of strong global agreements, leaving cybercriminals and so-called "hacktivists," whose motives may not be financially motivated, to operate in jurisdictions of their choice.
- **Response strategies are evolving.** Because of the changing nature of cybersecurity, financial institutions are forced to constantly monitor the threat landscape and determine both their potential likelihood and impact in order to prioritize their responses. In this effort, there has recently been a shift in thinking: from trying to prevent all risks, to instead trying to identify key weaknesses. To do so, many financial services institutions leverage data and look for trends in order to pre-empt potential attackers. Those who are particularly successful also establish key performance indicators (KPIs) based on such data, translating this from technical jargon to business terms that management can understand. In this effort, there is a growing realization that cybersecurity must also move from being seen as a technical problem toward a broader, risk-based approach.

- **There is a growing need to better harness data analytics.** Financial institutions currently live in a reactive world in which they conduct forensic analysis on their systems, data and networks to determine where weaknesses may persist or where threats or breaches have occurred. But this is an increasingly outdated approach, given that data volumes are growing rapidly and the threats are becoming ever more complex to analyze. As recently uncovered through the widely reported Edward Snowden leaks, governments have long used analytics to sift through massive amounts of data in order to improve security and anticipate future events. In order for financial institutions to become proactive, they too must harness their big data assets and utilize high-performing analytics to facilitate risk-based responses to potential incidents.

Introduction

Dependence on information and communications technologies (ICTs) has increased rapidly, as have the consequences of disruption. In the United Kingdom, the 2010 *National Security Strategy* says cyberattack is one of the four highest risks facing the country.[1] In March 2013, the United States identified it as the greatest threat to national security, surpassing terrorist groups such as al-Qaeda.[2]

Cybersecurity affects us all and even seemingly mundane cyberincidents can have major ramifications. In April 2013, for example, a hijacked Associated Press Twitter account was used to announce that bombs had exploded at the White House, injuring President Barack Obama. Although the tweets were retracted within minutes, the market plunged $136.5 billion on the news.[3]

Similarly, the opportunities created by ICTs are also a particular challenge for financial services institutions. As they continue to innovate in finding and introducing new ways to reach customers, they simultaneously expose themselves to new risks. Although cybersecurity is a wide-ranging problem affecting multiple industries, this report looks at the challenges and opportunities specifically as they relate to banking institutions, and the factors that affect them.

One example is the rising complexity of cyberthreats: Attackers circumvent secure banks by targeting weaker links in the information supply chain. “The biggest change coming is a shift from primary targets, which from a criminal point of view has been banks,” says Mike Usher, Director of Information Risk at Prudential Corporation Asia, a financial services firm. “But vigorous investment [at banks] has opened up secondary targets, which in the crime world might be insurance companies or anyone who holds significant information on customers.” The proliferation of attack targets means that banks can no longer protect customers by simply securing their own online assets.

1 http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

2 http://edition.cnn.com/2013/03/12/us/threat-assessment

3 http://www.abc.net.au/news/2013-04-24/ap-twitter-feed-hacked/4647630

"Organized crime groups will try you across channels. They don't care whether it's online; they look for the weakest link," agrees David Pollino, Senior Vice President and Enterprise Fraud Prevention Officer at Bank of the West, a retail and commercial bank based in San Francisco, US.

"This can be a challenge for third parties as well as small to medium-sized banks, which are particularly vulnerable once criminals understand their weaknesses," says Brian Lapidus, Senior Vice President and Practice Leader at Kroll Advisory Solutions, a risk firm. In the survey conducted for this report, 30 percent of respondents from smaller banks (those with global annual revenues of $500 million or less) said their main challenge has been a focus on individual risks rather than taking a holistic approach, compared to only 11 percent who say so at large institutions (revenues of $5 billion or more).

To deal with the challenge, banks and the stakeholders they interact with must enhance their understanding of cyberthreats, as not all crimes should be treated equally. "It's an evolution on how to think about the problem," says Lapidus. "On the bank side, we see them focusing on vulnerabilities more so than looking for proactive remedies." In this effort, growing data volumes are at the center of both the problem and the potential solutions. In order to get proactive and make risk-based decisions, leading organizations look to data management and analytics, which can help them better anticipate the nature of threats and determine the most appropriate action to meet them. The recent leaks by Edward Snowden, an American computer security contractor who exposed US government activities in collecting and analyzing big data, shows that governments have long used such approaches to gather intelligence. Now, leading financial institutions are looking at similar techniques to predict the threats that they face.

In order to better understand the threats facing banks, this report begins by identifying the scope of the cyberrisks faced today, before delving into particular challenges, responses, and ways forward.

Part I: Cyberrisk

Cyberattacks are both common and costly to consumers and companies alike. According to the *2012 Global Financial Services Industry Security Study* from Deloitte Touche Tohmatsu Limited, an accounting and consulting firm, about one-quarter of all banks were victims of a cyberbreach in 2011.[4] Meanwhile, the *2012 Norton Cybercrime Report* from Symantec, a security company, estimates the global annual cost of cybercrime to consumers to be about $110 billion.[5] Our survey findings for this report reflect this reality. Although low-level issues such as spam are fairly universal, other concerns are high: One in two banks report being a target of a phishing event in the past two years, while more than one in three have been affected by both malware and mobile malware (see chart 1). Just 6 percent of those polled say they have not been the target of some kind of cyberincident, broadly defined, over this period.

[4] http://www.deloitte.com/view/en_GX/global/176ea3aa991b9310VgnVCM1000001a56f00aRCRD.htm

[5] http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

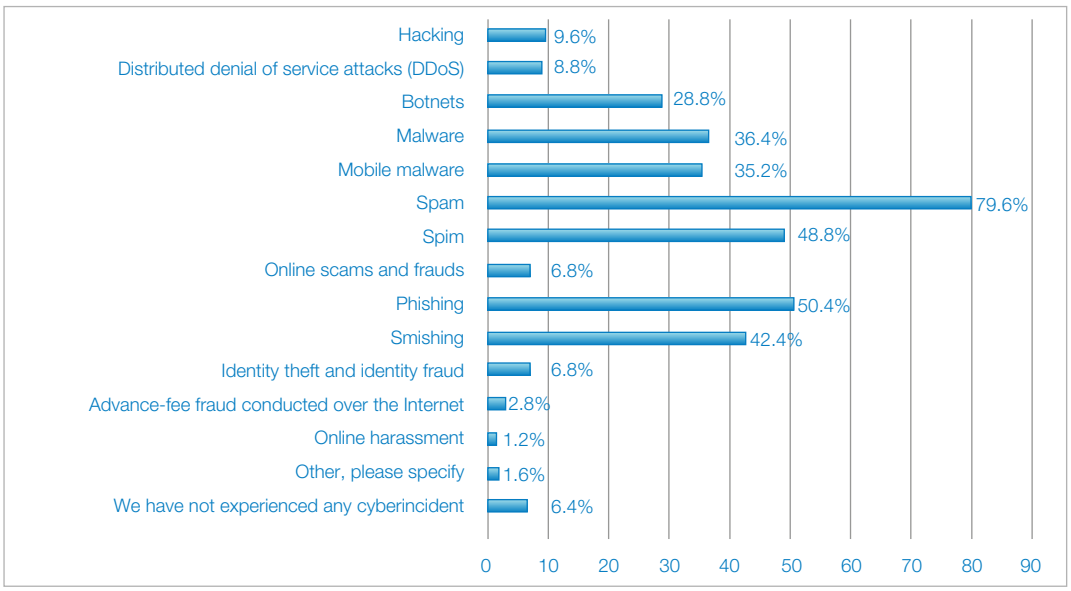

Chart 1: Proportion of banks that have been targeted by any of the following cyberincidents in the past two years

Furthermore, it is clear that the risk is rising. Nearly twice as many of the 250 banking executives polled expect cybersecurity to pose a "significant" risk to their organization in the coming two years as compared to today (74 percent, versus 38 percent now). More than three-quarters (82 percent) also think the rate of increase of financial losses from cyberattacks is rising at an unacceptable rate. The survey reveals that their organizations have experienced a wide variety of cyberincidents over the past two years. Spam, spim (the mobile version of spam), malicious software (malware), mobile malware, phishing and botnets are just some of the most commonly cited incidents.

But not all cyberthreats are of equal concern. When combining the likelihood and impact of various crimes (see chart 2), certain types of threats stand out. Phishing, for example, which is a technique used to get unsuspecting users to provide information about themselves that criminals then use to access their accounts, is seen as having the highest impact on banks, combined with a high likelihood of attack. This is clearly more worrying for pure retail banks: 59 percent of retail bank executives reported incidents of phishing, compared with 40 percent of commercial bank executives.

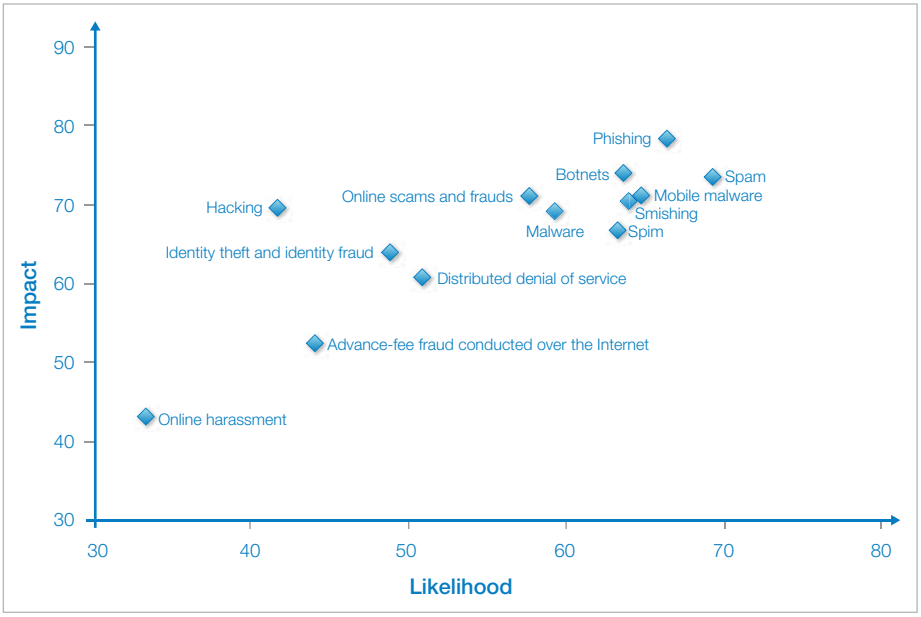

Chart 2: Risk radar: identification of most likely risks and most severe risks

Distributed denial of service (DDoS) attacks, which seek to block access to websites or online services, often garner great media attention but appear to be of less concern to banks. This is likely because the threat is primarily designed to cause disruption, rather than to steal money. About three-quarters (72 percent) of respondents also say they are seeing an increase in the political dimension to the threats faced. According to one interviewee, this introduces a new set of worrying threat vectors, generally described as "hacktivism." The motives are primarily to inflict reputational damage and call for attention to an issue, rather than looking to steal money per se. "Traditionally we don't have state-sponsored attacks against financial services," says Bank of the West's Pollino. "This takes it to a whole new level, which goes beyond financial services."

For example, in an annual report to the Securities and Exchange Commission (SEC), major banks in the United States acknowledged that they were targets of such attacks, which American officials believe were conducted by Iran in retaliation for sanctions connected to that country's nuclear program.[6] Such attacks have an impact on banks all over the world, given the global nature of these threats. In March 2013, for example, a number of financial institutions in South Korea were also targets of DDoS attacks, purportedly carried out by North Korea, rendering online services unavailable for several days, something which also occurred in 2009 and 2011.

[6] http://articles.washingtonpost.com/2013-03-01/world/37371617_1_private-sector-network-security-fifth-third-bank

Evolving technologies and threats

The ongoing evolution of technologies leads to a rapidly changing threat environment. This is a key issue. When asked what they see as their organization's primary challenges in dealing with cybersecurity in the coming two years, respondents rate technology limitations (cited by 39 percent) and difficulties in keeping pace with rapidly changing cyberrisks (38 percent). This is concerning because as the risk radar (chart 2) illustrates, threats are seen as having widely differing impacts and organizations currently appear to be catching up in using the latest technologies to mine their data proactively. There is definitely a learning curve in keeping up with the latest threats as they are constantly evolving and changing," agrees Lapidus. In this effort, organizations need to better leverage technology, monitoring solutions and analytics to identify potential vulnerabilities, incidents and their impact, which can enable organizations to take a more risk-based approach.

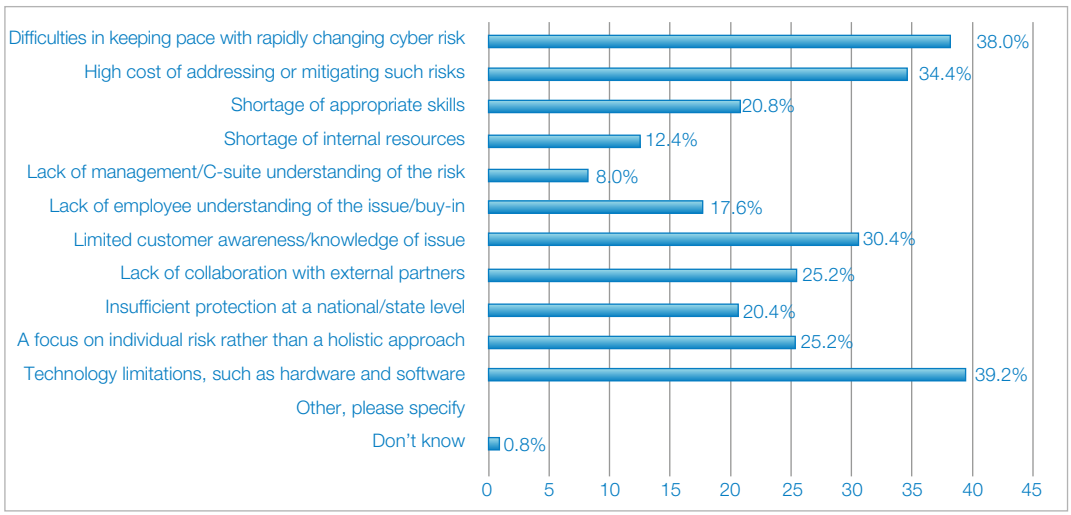

Chart 3: Key challenges in dealing with cybersecurity threats

Besides probing for the weakest link in the banking ecosystem, criminals are also developing new methods of attack and target new channels of communication as banks introduce them. For example, the user-friendly VISA payWave system, in which a customer simply swipes a card near a reader to buy something, makes it far faster and more convenient to pay, but also exposes the transaction to unauthorized users who can steal the information wirelessly. "I don't believe it's been thought through," argues Richard Frank, a member of the International Cybercrime Research Centre at Simon Fraser University in Canada. "It's easy to use but also easy to steal." As one example, he highlights a YouTube video that shows a person walking around a mall asking people for directions while holding a device that captures their credit card information. This highlights the difficult balancing act that banks and payment card providers face, between user-friendliness and security.

While evolving technologies provide new customer service opportunities, they also expose banks to more complex methods of attack. A particularly striking example is the introduction of mobile banking and mobile applications. These offer customers far more convenient channels for communication; equally, mobile threats such as mobile malware and spim are also among the fastest growing forms of cyberattack. According to the *2013 Internet Security Threat Report* from Symantec, there was a 58 percent increase in mobile malware compared with a year earlier, and a 32 percent increase in the number of reported vulnerabilities in mobile operating systems during the same time frame.[7] "Mobile is growing faster than any other banking service," says Pollino. "You have to embrace it but you have to balance usability with security."

This is a tough trade-off, as Danske Bank, a Danish retail bank, found out. When it introduced its mobile banking app in Sweden, it required users to use security tokens to access any services – a highly secure, but far less convenient way to get information. Its app was subsequently rated a poor 1.5 out of 5 stars in the Apple App Store℠ by users. But after analyzing usage data, Danske Bank realized that most customers actually just wanted to see their account balances, says Poul Otto Schousboe, the bank's Head of Group IT Security. Accordingly, Danske Bank allowed customers to simply use their static pin codes for account balances, while still insisting on a token for any account transactions to ensure safety there. Customers immediately responded to the added convenience and within a few days the app's rating leaped to 4.8 stars.

This also highlights a related balancing act that banks have to perform, between ensuring that financial losses don't get out of hand and retaining high levels of trust from customers in the services provided. Customers want both convenience and security, but it is up to banks to find the best trade-off, as the example with Danske Bank demonstrates. Indeed, our survey highlights that while financial losses have had a significant impact of cyberattacks in the past two years, a loss of customer trust is far more worrying, with nearly twice as many banks citing this as a significant impact (see chart 4).

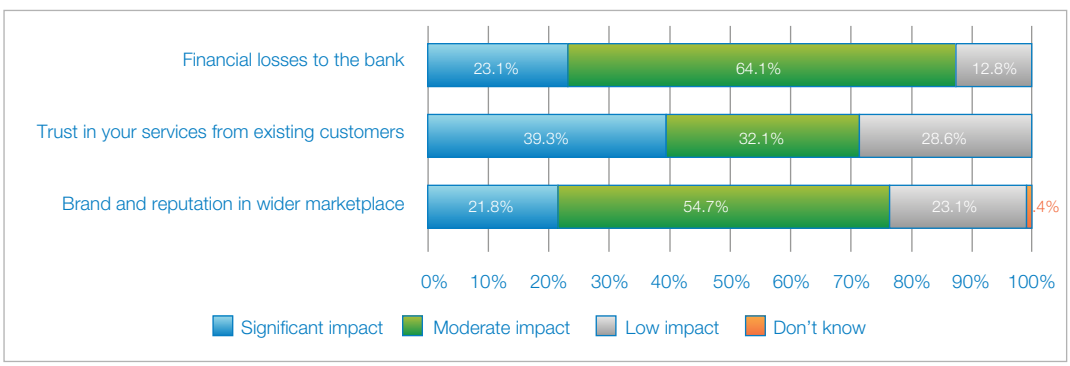

Chart 4: The degree of impact from cyberattacks on key aspects of a bank's business

[7] http://www.symantec.com/security_response/publications/threatreport.jsp

Lack of awareness

Lack of disclosure leads to lack of awareness, another key challenge to cybersecurity. About three-quarters (77 percent) of survey takers say customer knowledge and understanding of cyberthreats is simply not keeping pace with market developments; in fact, it is rated as the fourth biggest challenge in the next two years (cited by 30 percent). As a result, 70 percent of respondents also say they must impose additional security measures on their customers – either via software or hardware.

This can range from simple image verification, in which customers are prompted to identify a picture in order to make transactions, to more complex solutions such as personal security tokens. In Denmark, for example, banks use a single sign-on solution called NemID, which is shared with public sector services, such as tax, health care and insurance.[8] Although secure from a communications perspective, the reliance on a single solution for the entire population can also prove problematic. On several occasions, most recently in April 2013, large-scale DDoS attacks have rendered many services unavailable. Although backup systems limit the magnitude, this can still prove disruptive.

To improve customer relationships while simultaneously educating them on security risks, banks must embrace all lines of communication, notes Bank of the West's Pollino. His firm actively monitors online content and leverages social media channels for real-time communications as needed.

Besides external education, there is also a need for raising internal awareness. Indeed, "human behavior" is often cited as a key gap in cybersecurity among banks. Unless properly and consistently trained surrounding security protocol, employees are often careless about their use of USB devices and public Wi-Fi connections as examples of various vulnerabilities that occur, says Kroll's Lapidus. Danske Bank, which has over 20,000 employees across almost ten countries, has learned from experience. For example, when the bank started to introduce laptops to employees, it also made sure they were all encrypted. Part of the success of such initiatives, adds Schousboe, is attributed to the fact that management is keenly aware of and interested in security. Today it continues to encrypt all devices connected to its network.

[8] https://www.nemid.nu/dk-da/om_nemid/about_nemid/

But this is not the case at all organizations. Indeed, lack of awareness among senior executives is common, for a variety of reasons. Despite rising threats, more than half (54 percent) of survey respondents say their organization's financial losses from cyberattacks are not high enough to warrant board-level attention, leaving senior management unaware of the potential problem. This is partly because most organizations handle security as an extension of IT rather than viewing it as an operational risk, says Chris Smith, Director of Service Engagement and Federal Enterprise Architecture at SAS. For example, although many organizations today have a chief information security officer (CISO) or similar position, they primarily report to the chief information officer (CIO), viewing the problem as a technical one. "But the CIO needs to continue the evolution of cybersecurity into a broader risk issue," says Smith.

Case study: The DNA of a 21st-century ATM heist

Criminals are constantly developing new methods to attack traditional channels. One such incident in early 2013 was anything but conventional, and appeared more like the plot of a Hollywood film. In a highly coordinated attack involving people across some 20 countries, cybercriminals worked with local groups to manipulate financial systems and magnetic strips on debit and credit cards to steal $45 million from thousands of ATMs around the world during two separate attacks. While an ATM heist is an age-old crime, the methods deployed were wholly from the 21st century. What follows is a breakdown of how it happened:[9]

1) *Targeting a specific product*
   Hackers identified prepaid debit cards from Visa and MasterCard as their primary targets because such cards are preloaded with money instead of being linked to specific accounts, thus minimizing early detection.

2) *Identifying the weakest link*
   The global financial system is only as strong as its weakest link. In the first operation in December 2012, hackers infiltrated an unnamed Indian credit card processing company to steal card information; in the second operation in February 2013, they targeted an American credit card processing company.

3) *Raising the scope*
   Instead of using the stolen data, the hackers raised the scope of the attack by increasing or removing the withdrawal limits on the prepaid cards by infiltrating the National Bank of Ras Al Khaimah in the United Arab Emirates during the first attack and the Bank of Muscat in Oman during the second attack.

4) *Executing the plan through global coordination*
   Account information was sent by the hackers to local crews in about 20 countries around the world, who used the data to program the magnetic strips of cards in order to withdraw money from them on local ATMs.

[9] Sources for this include: http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?_r=0, http://money.cnn.com/2013/05/09/technology/security/cyber-bank-heist/index.html, and http://www.bbc.co.uk/news/world-us-canada-22470299

5) *The heist*
In December, local crews used five account numbers to make 4,500 transactions worth $5 million. In February, they used 12 account numbers to make 36,000 transactions worth $40 million.

6) *Laundering the money*
Local crews used the money to purchase luxury items, including Rolex watches and cars, in an effort to launder the money. They also deposited some of the money into bank accounts – presumably those of the hackers. In one instance as much as $150,000 was deposited.

The bottom line: this 21st-century ATM heist illustrates the growing complexity of the threats facing financial institutions. In order to understand their adversaries, banks must anticipate new, sophisticated forms of attack, or new versions of old tricks. At the same time, they must also work to ensure that their partners and stakeholders are secure, as part of strengthening the entire supply chain of information to minimize attacks against the weakest links. They must do all this while simultaneously rolling out services across emerging channels, such as mobile. It is a challenging task, but vital if customer trust is to be maintained.

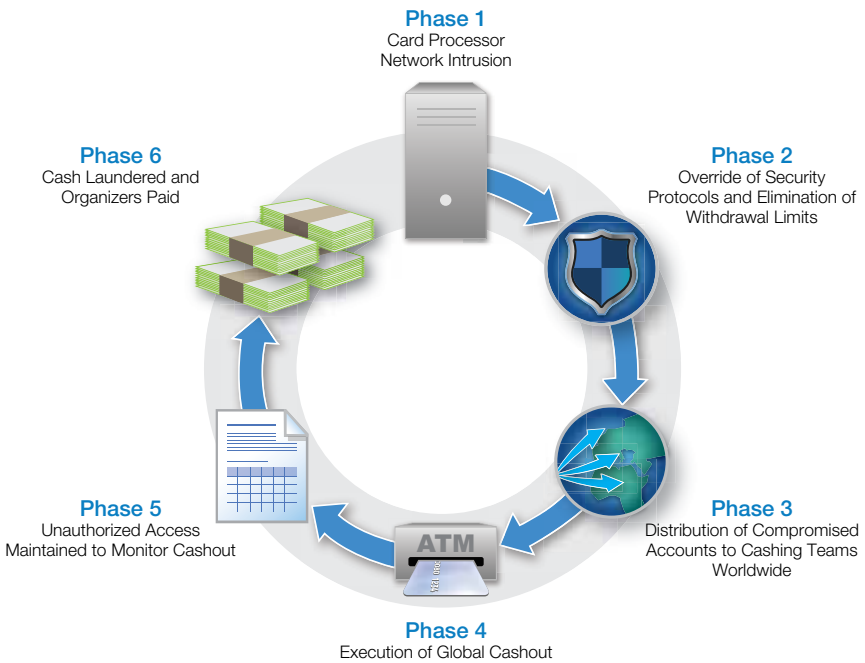

Figure 1: The DNA of a 21st-century ATM heist

Part II: Cyberresponses

As the nature and severity of cyberrisks increase, what does this all mean for banks in terms of how they respond? First off, it is clear that banks are now forced to constantly monitor the threat landscape and determine both the likelihood and potential impact in order to prioritize their response. This is challenging. “The learning curve is very steep and the landscape is dynamic and complex,” notes Adel Melek, Managing Director for Global Enterprise Risk Services at Deloitte Touche Tohmatsu Limited. “Furthermore, you don’t have a whole lot of time to understand, evaluate and analyze.”

The rise in vulnerabilities combined with limited response time has spurred banks to realize that no organization is, or can be, 100 percent risk free. As a result, there is a shift in mindset underway, from a focus on trying to prevent all possible risks, to instead identifying key weaknesses and mitigating those. “We have to help the business side understand that there is a difference between a relative risk and an absolute risk,” explains Prudential’s Usher. “A lot of IT issues are risks that should be made relative to other business risks. If it’s a huge risk, then make it relative to other risks and don’t oversell it,” he advises.

“Banks follow risk prioritization strategies while trying to predict high potential threats,” says Melek. For him, cyberthreat intelligence consists of two key parts. First, organizations must be able to aggregate both external and internal threat intelligence in a way that is meaningful and relevant, including the ability to filter it. Second, organizations must be in a position to act on it. “We are seeing a high degree of adoption of analytics among larger banks,” he says. “Information security is a perfect candidate for big data and analytics.”

“Having good data is absolutely critical,” says Bank of the West’s Pollino, who notes that his firm is investing a lot to analyze information and transform it into key performance indicators (KPIs). The aim here is to better leverage limited resources while enhancing understanding of different threats.

In this area there has also been an evolution from complex measurement toward a more holistic risk-based approach. At Prudential, Usher used to have a 150-question survey that more than 20 business units across more than 10 countries completed. Today, he has simplified and consolidated it into 50 questions. “It’s the biggest evolution and we turned it from an information security questionnaire with very detailed information into a business risk-focused questionnaire,” he says.

Based on his experience, Usher recognized that technical cybersecurity terms simply didn’t resonate with board committees and senior management. “What we’re doing now is to move away from technical terms to communicate better internally but also externally.” To do so, he is working to transform the KPIs derived from the new survey questionnaire into business language that management can understand. “We have to simplify things so the business side can understand the problem.”

Breaking down such internal barriers between the information security and business functions is also one of three major trends this year, as reported by the *2012 Global Financial Services Industry Security Study* from Deloitte.[10]

Case study: Lessons learned

Just as cyberthreats are constantly evolving, so too are the lessons learned. Initial approaches to solve the problem came from technical solutions, such as antivirus and later firewalls. This might be one reason that organizations continue to handle cybersecurity as an extension of an IT problem rather than a broader operational risk issue. In the evolution of such thinking, interviewees pointed to a number of continuing problems from which lessons can be learned, across several consistent themes. They include:

The human factor. People are both the problem and the solution for much of cybersecurity. Insiders are a particular threat, as is "human error," which Deloitte's Melek notes as a persistent issue across geographic regions. To deal with it, some suggest better employee training, limiting administrative rights on workstations and improving consumer knowledge. "There is never enough customer awareness and there are lots of evolving methods, particularly social media," says Kroll's Lapidus.

Lack of strategies or ineffective policies. Although many companies now have high-level strategies in place, many ineffective policies, or policies that are simply not enforced, still persist. Instant response plans that are "comprehensive and written" are often recommended. In this effort, institutions should define the risks and prioritize them according to their impact. In line with this report's risk radar (see chart 2) some threats must be prevented as strongly as possible, whereas others may simply be an acceptable cost of doing business. In addition, cyberstrategies should include a stronger focus on incident response, such as who will deal with media inquiries when there is a breach.

Inadequacy of budgets and resources. Lack of support can be attributed to both lack of awareness among top management and the need to spend only enough to make consumers trust a bank. However, when an incident occurs, this can be a wake-up call. In 2003, Danske Bank suffered from a series of software and hardware failures, which effectively shut down operations for almost a week.[11] But the good news is that management learned from the incident, says the firm's Schousboe, and the bank now invests more heavily in maintenance and disaster recovery control.

Measurable KPIs. Despite its obvious benefits, interviewees note a lack of key risk indicators, which would put organizations in a better position to accurately measure the extent of the threat and their own weaknesses. Danske Bank runs weekly assessments and its yearly disaster controls and tests are communicated to the highest levels of the organization.

[10] http://www.deloitte.com/view/en_GX/global/industries/financial-services/42a6436f82559310VgnVCM2000001b56f00aRCRD.htm#

[11] http://www.computerweekly.com/feature/DB2-failure-prompts-bank-to-set-up-extra-disaster-recovery

Trust trumps financial losses

Achieving strong cybersecurity preparedness requires good technology, the right organizational structures, strong cooperation, legal support and investment. However, as the first section of this report highlighted, concern over customer trust clearly takes greater precedence for banks than financial losses. In fact, when considering which impacts from cyberattacks were most significant, customer trust was rated nearly twice as high as monetary losses.

In assessing all of these, the weakest link within banks relates to a lack of internal resources devoted to cybersecurity. Only 24 percent of survey respondents say they are "highly prepared" in this area, followed by 32 percent who cite external cooperation. In both instances, more than one in 10 flag either limited preparedness or a lack of preparedness overall (see chart 5).

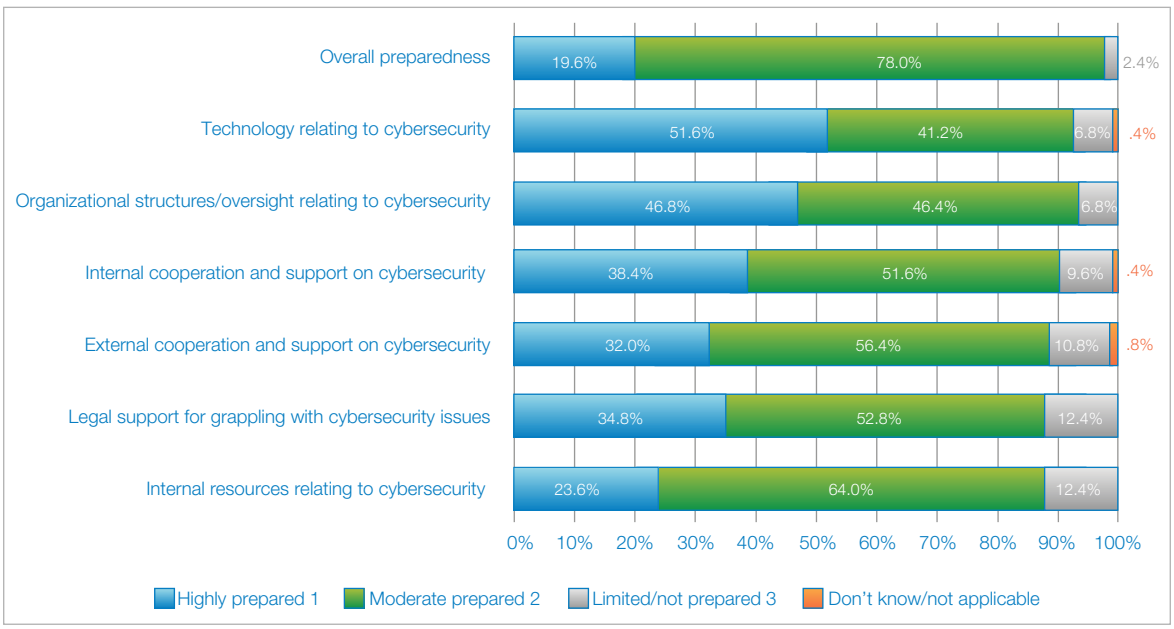

Chart 5: The degree of preparedness for cyberrisks within banks today

The lack of internal resources may be because banks approach cybersecurity from a return on investment perspective, spending whatever it takes – but only just enough – to ensure sufficient security to make consumers trust them. In fact, 84 percent of survey respondents agree that their organization will spend whatever it takes to secure online channels in order for consumers to trust them.

"Financial services are built upon trust from our clients, trust between our firms and the trust required to ensure the proper functioning of markets, execution of transactions and protection of information," explained Charles Blauner, the chair of the Financial Services Sector Coordinating Council (FSSCC), in a written letter to the National Telecommunications and Information Administration in April 2013.[12] Danske Bank's Schousboe adds that security has not been an area of competition among banks in his country. "If something happens, there is a loss of trust to the entire industry," he says.

Indeed, whereas direct financial losses appear tolerable for many banks today, a driving factor behind increased spending is trust. Indicative of this, almost three-quarters (72 percent) of survey respondents say their budgets for dealing with cyberrisks will rise in line with the expanding scope of the threat. As one interviewee puts it, at the end of day, it's all trust-related as financial costs are passed on to consumers anyway.

A lack of cooperation

Although many banks appear concerned about the potential increase in high-profile attacks, they still largely operate in silos, both internally and within the wider finance sector. "There isn't a great incentive for them to be collaborative because they just have to prove that it wasn't their system that was compromised," explains Prudential's Usher. He points out that in practice, banks have contracts with both consumers and other third parties that limit their financial losses stemming from attacks outside of their systems.

As a result, it is unsurprising that nearly eight in 10 (78 percent) respondents say their bank does not rely on any other parties when it comes to coping with cybersecurity. Although many banks collaborate with each other to some extent through organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the US, which enables members to share information and receive early warning and expert advice, the industry as a whole still appears to largely operate in a silo.

The Financial Services Sector Coordinating Council in the US, for example, calls on the government to "step up the prosecution of cyberthieves at both the federal and state levels."[13] Nearly eight in 10 respondents also say national sentencing guidelines relating to cybercrime need to be toughened up to act as a sufficient deterrent to criminals (see chart 6).

[12] http://www.americanbanker.com/issues/178_82/best-incentive-to-shore-up-cybersecurity-trust-bank-group-says-1058708-1.html

[13] http://www.americanbanker.com/issues/178_82/best-incentive-to-shore-up-cybersecurity-trust-bank-group-says-1058708-1.html

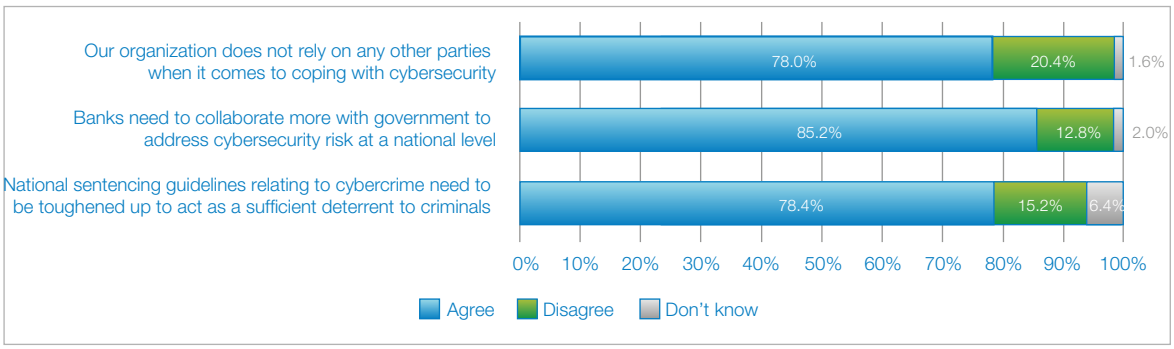

Chart 6: Proportion of respondents who agree or disagree on the following statements

The problem is compounded at the global level. Because of the international dimensions of cybersecurity, which often require cooperation between law enforcement agencies around the world, deterring and finding criminals is often a daunting, if not impossible, task. Even prominent international agreements, such as the Convention on Cybercrime (also known as the Budapest Convention) have only garnered 39 signatories around the world, leaving criminals to operate in a number of countries that have yet to participate in international cooperation in this area. "These crimes can be committed from anywhere and we need to establish greater cooperation globally to make it dangerous for criminals," says Richard Frank of the International Cybercrime Research Centre.

Conclusion: Key actions ahead

The cyberdomain is constantly evolving, providing both new opportunities and challenges for financial services institutions. "We have a velocity problem, a volume problem and a value problem, and the industry is still trying to figure out what's important," says SAS' Smith. To improve cybersecurity, financial services institutions, like many other organizations, must elevate the topic and address threats holistically to the highest levels of the organization in a manner that they understand. In this effort, they need to:

- **Understand threats.** Just as the likelihood and impact of cybercrimes varies, so should the responses to them. In this effort, banks need to distinguish between financially motivated attacks and those that are non-financial in nature.
- **Cooperate externally.** Banks are perceived as operating in silos, but greater external cooperation should enhance their cybersecurity efforts more broadly. Criminals often target weaker links in the banking ecosystem, and it would be in the banks' long-term interests to help third-party actors improve their own cybersecurity efforts.
- **Improve awareness.** Greater communication between the technical and business functions is necessary to improve cybersecurity within enterprises. By educating everyone from end users and employees to top management, banks must continue to improve educational efforts surrounding cybersecurity.

- **Leverage data assets with advanced analytics.** Like many organizations, banks have enormous amounts of data at their disposal, which they can leverage with analytics tools to detect trends and create KPIs from which to proactively counter cyberthreats.
- **Take risk-based decisions.** Taking a holistic view of cyberthreats requires an elevation of the problem to an operational risk, from which better decisions can be taken faster and in relation to the relative risk to the enterprise as a whole.

In the effort to meet the cybersecurity challenge, banks will be helped by evolving technologies too. New tools are rapidly emerging to fill existing gaps in both reactive forensics, such as e-discovery solutions, and proactive analytical tools, which can mine significant data sets to analyze patterns and support risk-based approaches to managing risk. This use of so-called “big data” is only valuable if it can be properly analyzed and provide a sound basis for making better decisions. This is particularly relevant for cybersecurity, as not all threats are equally severe and must be prioritized accordingly. Implementing analytics can help financial services institutions better understand what, when, why and how threats can potentially have an impact on an organization, and how they can determine the most appropriate action to meet the challenges ahead.

THE POWER TO KNOW.

SAS Institute Inc. World Headquarters +1 919 677 8000
To contact your local SAS office, please visit: **sas.com/offices**