Deloitte.
University Press

Taking cyber risk management to the next level

Lessons learned from the front lines at financial institutions

About the Deloitte Center for Financial Services

The Deloitte Center for Financial Services, part of the firm's US financial services practice, is a source of up-to-the-minute insights on the most important issues facing senior-level decision makers within banks, capital markets firms, mutual fund companies, investment management firms, insurance carriers, and real estate organizations.

We offer an integrated view of financial services issues, delivered through a mix of research, industry events, roundtables, and provocative thought leadership—all tailored to specific organizational roles and functions.

CONTENTS

Rising to the cyber risk challenge | 2

Money is no object: An embarrassment of riches for cyber risk management | 6

CISOs stuck between a rock and a hard place while juggling multiple priorities | 8

CISOs striving to innovate while struggling with new tech tools and organizational transformation | 11

Cybersecurity starving for “triple-threat” talent | 16

Risk metrics remain a Tower of Babel as reporting responsibilities overwhelm CISOs | 20

CISOs need help connecting the dots with intelligence sharing and analytics | 23

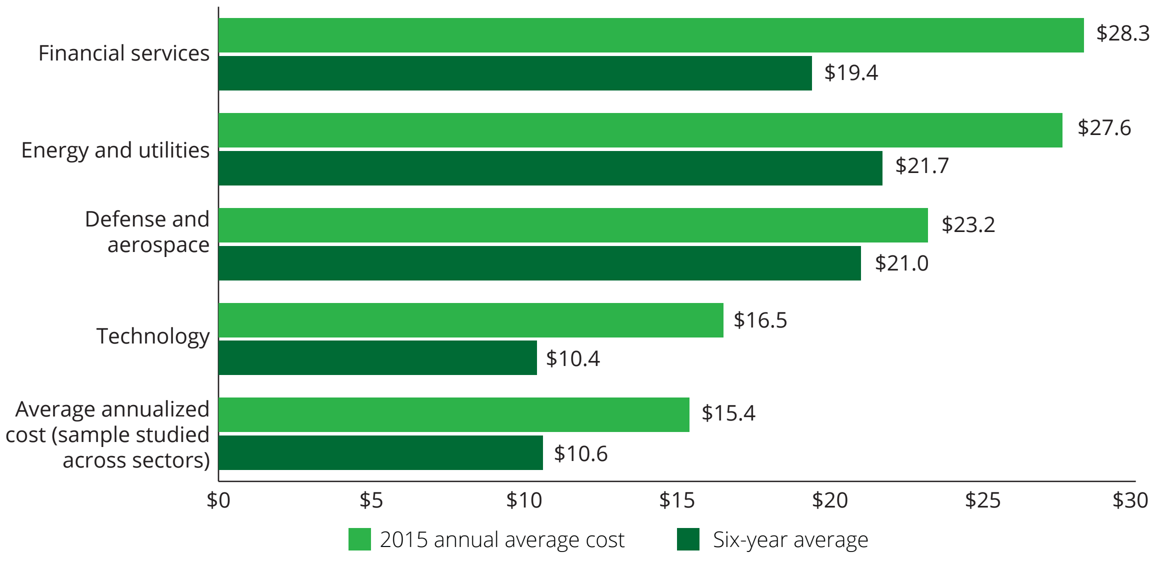
Looking ahead: No rest for the weary in cyber risk management | 25

Endnotes | 27

Rising to the cyber risk challenge

BANKS, investment companies, and insurers are prime targets for cybercriminals looking to steal money or information, disrupt operations, destroy critical infrastructure, or otherwise compromise data-rich financial services institutions (FSIs). Indeed, FSIs lead the pack in terms of the average cost of cybercrime incurred by companies in a particular industry, counting both internal activities and external consequences. That figure reached $28.3 million in 2015—which is significantly higher than the six-year average for FSIs of $19.4 million annually (see figure 1).[1]

Figure 1. Average annualized company cost of cybercrime (by sector, $ millions)



Source: Ponemon Institute and Hewlett Packard Enterprise, *2015 Cost of cyber crime study—United States*, October 2015.

Graphic: Deloitte University Press | DUPress.com

There's no shortage of money or technological tools being devoted to support cyber risk management at FSIs, as such threats are high on the agendas of senior management and board members. Cyber exposures rank second only to regulatory/compliance concerns as the types of risks FSIs believe will increase the most in importance to their companies.[2] At the same time, only 42 percent of those responding to the most recent Global Risk Management Survey by Deloitte & Touche LLP feel that their organization is "extremely effective" or "very effective" in managing cyber exposures.[3]

Yet despite having had several years to bolster cybersecurity capabilities, our latest research found that many FSIs are still struggling to keep up with a moving target. Basic blocking and tackling strategies to lock down devices, systems, and platforms remain a work in progress at many companies because of the pace of attacks, the growing sophistication of threat actors, as well as multiplying, often conflicting demands facing chief information security officers (CISOs).

Adding to the sense of urgency surrounding cybersecurity is the massive technological transformation underway in financial services driven by fintech, regtech, mobile applications, cloud adoption, and other emerging developments. CISOs and the business executives they work with are being challenged to become more agile and provide a frictionless customer experience. Beyond facilitating technology upgrades, they must balance the needs of cybersecurity with other forces, such as cost reduction, globalization of the workforce, and regulatory compliance.

To get to the bottom of these challenges, the Deloitte Center for Financial Services conferred with cyber risk experts from Deloitte Advisory about the state of security, vigilance, and resilience efforts at banks, insurers, and investment companies. We then interviewed senior cybersecurity, technology, and risk management specialists from across the industry to learn more about their first-hand experience and strategies. Those interviewed shared cyber war stories from the front lines, citing a wide variety of obstacles and frustrations, as well as the progress they've made and plans to transform their thinking, approaches, and organizational culture going forward.

> Cyber exposures rank second only to regulatory/compliance concerns as the types of risks FSIs believe will increase the most in importance to their companies.

Our interviewees did not always echo one another in terms of their number-one challenge, which cybersecurity investments had paid the biggest dividends, or even their future priorities, mainly due to their varying levels of risk management maturity and differences in the FSI sub-sectors they inhabit (see "CISOs cite wide range of challenges, investments" on page 4). However, there were a number of key areas of consensus among those who took part in the research. Several broad themes emerged, which we'll explore in more detail:

- **Money is no object for those we interviewed, with cybersecurity budgets rising dramatically over the last few years.** However, most agreed that the pace of such increases is not likely to be sustainable over the long run, meaning some hard choices will soon have to be made in terms of priorities.
- **The majority feel stuck between a rock and a hard place as they juggle multiple priorities.** They are being challenged to address vulnerabilities within a plethora of legacy systems. They are expected to innovate via the cloud, fintech, digital identity, and additional breakthroughs even as they struggle to keep basic systems up and running. All the while, they are trying to align cybersecurity policies and

efforts with the business, operational, and technology strategies of their companies.

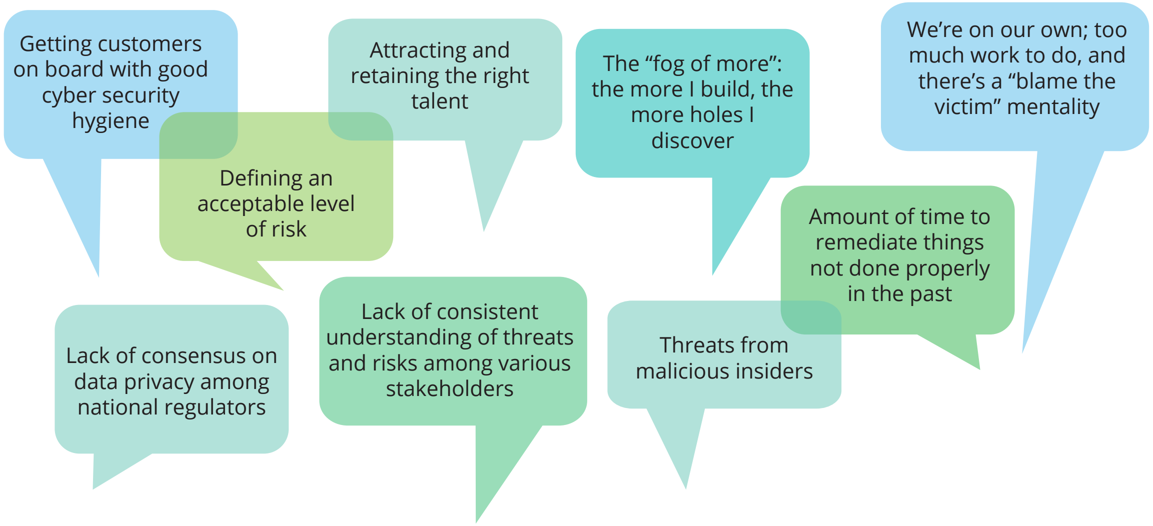
- **CISOs are striving to innovate in a multitude of ways**, but often have a hard time assessing and integrating a flood of new security tools at their disposal, while reinventing their organizations to make cybersecurity a core consideration enterprise-wide.
- **FSIs are starving for cybersecurity talent**, with staffing challenges the biggest problem faced by many of those we interviewed. While companies may have more than enough

CISOs CITE WIDE RANGE OF CHALLENGES, INVESTMENTS

While this report is focused on areas of consensus among those we interviewed from major financial institutions as to the current and future state of cyber risk management in the industry, it's worth mentioning they did not always march in lock-step. That's not surprising, given the varying levels of maturity and industry sector dynamics among our relatively small but representative group of CISOs.

For example, when asked about the most important challenge they feel their organizations are facing, the responses largely reflect the main points covered in the body of this report, with some interesting exceptions, as shown in figure 2.

Figure 2. There appears to be a lack of consensus on the most important cyber risk management issues in financial services today


Getting customers on board with good cyber security hygiene
Attracting and retaining the right talent
The "fog of more": the more I build, the more holes I discover
We're on our own; too much work to do, and there's a "blame the victim" mentality
Defining an acceptable level of risk
Amount of time to remediate things not done properly in the past
Lack of consensus on data privacy among national regulators
Lack of consistent understanding of threats and risks among various stakeholders
Threats from malicious insiders

Graphic: Deloitte University Press | DUPress.com

When it comes to return on investment (ROI) and future initiatives, our interviewees once again expressed a range of priorities. Banking CISOs maintained that improving their firm's resilience in the event of an attack is a future investment priority. In contrast, insurance CISOs cited network monitoring and identity management as priorities. Similarly, investment in "basic blocking and tackling" to remediate legacy systems was identified as an area that has paid off for bankers in particular, while other sectors were less consistent, mentioning talent, application consolidation, or data protection as high-return areas for their specific institution.

Clearly, the diversity of responses reflects the fact that even though financial services has been a main target of threat actors for many years, companies within the industry are still focusing on their own "next challenge"—building capabilities they hadn't prioritized before.

funding, they often complained about the lack of "triple threats"—those with the technical skills, business know-how, and strategic thinking capabilities to implement cyber risk management initiatives quickly and effectively.

- **Cyber risk metrics remain a veritable Tower of Babel** as reporting responsibilities overwhelm CISOs, thanks to a lack of widely accepted, impactful measurements and industry-wide standards to meet increasingly redundant oversight demands.

- **CISOs need help connecting the dots.** Many cite legal ambiguity or regulatory hurdles as obstacles to information sharing within and beyond the industry and even their home countries, while most yearn for ways to better automate intelligence to make it more relevant, actionable, and available in real time.

Overall, we found that while some FSIs have become leaders in cyber risk management, there is a wide variance on the cybersecurity maturity curve. The bar needs to be raised for many individual companies and the industry as a whole. Our interviews with leading players and experience in serving clients across financial services provide a number of key insights into how these challenges might be overcome, whether by sharing leading practices or through continuous innovation, just as the threat actors themselves have done.

Money is no object: An embarrassment of riches for cyber risk management

Where are FSIs now?

All of those we spoke with said their companies had dramatically increased cybersecurity budgets over the past few years, a trend they believe is likely to continue in the near term. For the time being, money appears to literally be the least of their concerns. One respondent said his cybersecurity budget had gone up 75 percent over the last three years, adding, “Money is simply not an issue.” Some noted they're often asked by superiors whether they don't need to spend more to combat cyber risk.

In addition, those we interviewed pointed out that an FSI's overall investment in cybersecurity is always higher than what's allocated in the CISO's budget, since spending is spread out among numerous departments. There are “hidden” cyber costs to consider, such as security-related expenses borne by application development teams, employee risk management training programs, the legal department, as well as related expenditures across the enterprise.

This enviable “money is no object” attitude at most FSIs reflects a recognition on the part of senior management and board members that cyber risks pose an existential threat to the organization, not only in terms of potentially huge financial and legal liabilities, but also considering the long-term damage that could be done to a company's reputation and market share. One executive said their budget had doubled since a competitor suffered a major breach, which served as “a real wake-up call” for his company. “That was a game changer for us.” As one CISO explained, if a substantial event occurs, a company doesn't want to regret its decision not to do something that, in retrospect, might have prevented or contained the breach, just to save money in the short run.

Where might FSIs go from here?

The bottom line is that by whatever measurement, cybersecurity is not being shortchanged by FSIs, and the vast majority of those we spoke with don't foresee a significant slowdown in spending anytime soon. One respondent said trends in cybersecurity spending are the “new normal,” noting that his budget will likely have to keep increasing to stay ahead of evolving threat actors.

But a number of interviewees acknowledged the pace of cybersecurity budget increases is unlikely to be sustainable over the long term. One respondent said outlays for security are “definitely on the rise, but not limitless.” Another predicted that he won't be able to justify higher and higher budgets “in perpetuity.” A third pointed out that while spending will continue going up for quite some time, he wants to at least bring down the rate of increase, and level it off, if possible.

But for now, the biggest budget issue is not the amount of money available, but the ability of CISOs to execute their strategies and communicate the ROI of their risk management programs. CISOs need to be able to have a dialogue with business leaders around ROI and demonstrate material risk reduction and/or risk avoidance. Communicating in simple terms the quantitative and qualitative benefits of cyber investments will be more important than ever as scrutiny increases.

CISOs will need to pay particular attention to managing a solution's lifecycle. Hindering this is the complaint by many that while they have the budget to deploy new tools and systems as needed, they often lack enough people with the necessary skill sets and capabilities for ongoing care and feeding of solutions to enhance their effectiveness. Execution speed is also greatly impacted by the inability to find and retain the necessary personnel in a highly competitive marketplace. Talent development and sourcing strategies are therefore going to require much more highly focused attention—a topic dealt with in more detail later in this paper.

Longer term, at some point CISOs will have to start making hard choices on spending priorities, based on a true cybersecurity game plan that is aligned with the company's business and technology strategies. Since it is probably unlikely, even for the largest institutions, to allot funds to build capabilities in all areas of security simultaneously, CISOs should triage among competing calls for investments. One interviewee advises his staff to be "disciplined" about product choices as new solutions emerge. CISO teams should see what works and what doesn't before adding or substituting new security technologies as they are introduced.

Beyond talent and technology, key areas that shouldn't be neglected at budget time include investments to create a cyber risk-aware culture. Many of those we interviewed have already initiated extensive and ongoing employee training programs to keep workers on their toes, such as virtual training and phishing tests, for example. However, we received consistent feedback that pure web-based instruction is not enough, with leading organizations using cyber war-gaming, red-teaming, and other table-top techniques to increase human, hands-on participation in training exercises. This process should also be extended to include education of third parties, including business partners, vendors, and customers—all of whom could be compromised to penetrate an FSI's systems.

TIPS FOR FSIs

- **Measure and communicate ROI**. Demonstrate quantitative and qualitative benefits of cyber investments.
- **Ensure lifecycle coverage.** Budget money not just for deployment but to keep solutions alive and effective for a number of years.
- **Don't neglect cyber talent development.** Invest to recruit, retain, and train the next generation of cyber warriors.
- **Don't shortchange cyber awareness programs and protocols.** Keep spreading the word beyond employees to vendors, business partners, and customers.

CISOs stuck between a rock and a hard place while juggling multiple priorities

Where are FSIs now?

Even though there is plenty of money available to combat cyber risks, CISOs say there is never enough time to address everything they are being asked to accomplish. Those we interviewed must juggle a multitude of responsibilities as they scramble to secure legacy systems and applications, contain a barrage of emerging threats, and establish a more proactive, innovative, and comprehensive cyber risk management strategy across their organizations. The burden can be daunting; one major FSI said his company faces between 5,000 and 6,000 attempted intrusions every day, estimating that about 1 out of every 20 people who access their systems is trying to steal something.

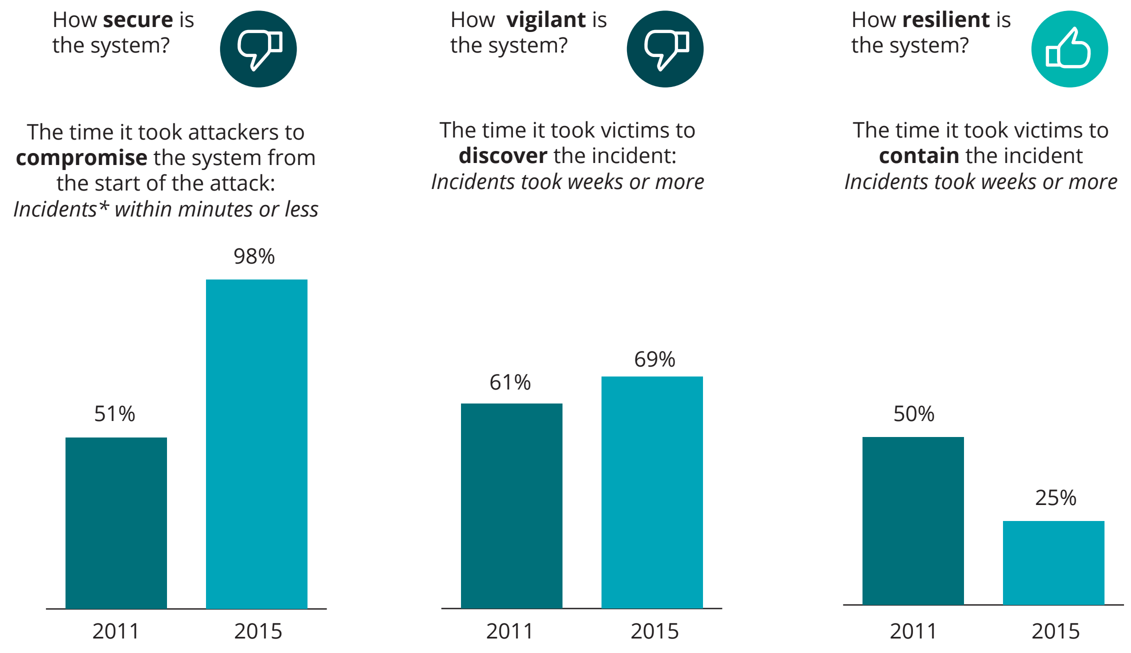
> A number of respondents described themselves functioning primarily for now as “first responders,” putting out a never-ending series of brush fires while trying to head off a cyber “inferno” that could take down the enterprise.

As a result, a number of respondents described themselves functioning primarily for now as “first responders,” putting out a never-ending series of brush fires while trying to head off a cyber “inferno” that could take down the enterprise. Many complained about being overwhelmed with basic legacy system remediation and compliance work when they’d prefer to be spending more time and money on broader, longer-term challenges—such as developing advanced analytics to better anticipate attacks. One respondent cited the “fog of more” as his biggest problem, noting that the more sophisticated his security detection program becomes, the more vulnerabilities he discovers that must be resolved.

Ideally, most respondents said they’d like to see a 50/50 split of their time and money between addressing the ongoing security needs of existing systems and those of new ones being launched, but the reality is that attending to legacy issues often accounts for a far higher portion of the budget pie. The goal should be to strike more of a balance between the two, so that security principles are built into new products, applications, and the like from the start, saving time, money, and effort to keep them safe from intruders later.

A big consideration is where a particular FSI is located on the cyber risk management maturity curve. Some we spoke with remain in the very early stages, spurred to ramp up quickly by a breach of their system or spooked by a major industry event. Others were facing challenges addressing security vulnerabilities in the aftermath of recent mergers and acquisitions. A handful were much further along the curve, having

Figure 3. Attacker's ability to attack vs. financial institution's ability to defend



*"Incidents" are cyber events that actually or could potentially compromise the integrity of a system's data or operations.

Source: Verizon, *Data breach investigations report (financial services)*, 2012 and 2016.

Graphic: Deloitte University Press | DUPress.com

created strong programs that continue to evolve with the threat landscape. However, while FSIs are improving their resilience in terms of how long it takes, on average, to contain an incident once an intrusion is discovered, there remains plenty of room for improvement when it comes to detecting breaches and preventing intruders from compromising their systems (see figure 3).[4]

Where might FSIs go from here?

This conundrum may never be fully resolved, as CISOs are continually called upon to up their games to meet the evolving cybersecurity challenge. However, most organizations can achieve a better balance among their multiple responsibilities by adopting more focused tactics and strategies.

First, respondents felt strongly that cybersecurity needs to be better integrated across the overall enterprise. This starts with having a cybersecurity strategy and roadmap that are aligned with those of business, operations, and information technology. It also means having an accountability model where multiple departments play a key role as part of the first line of cyber defense, so CISOs are not left fighting the battle on their own.

This effort could be facilitated by creating an oversight committee that includes the chief information officer, chief operating officer, chief risk officer, line-of-business (LOB) officials, legal representation, and other relevant stakeholders. Such a setup can provide the horizontal oversight necessary to drive cyber risk management deeper into the organization. This also allows for quick resolution of any disconnects between security and business leaders in terms of reconciling their respective goals and priorities. CISOs were loud and clear in emphasizing that they cannot be successful without business and IT co-owning responsibility in cyber solutions.

Second, proper pacing and monitoring are crucial to keeping everyone on the same page and moving forward together. One respondent's company had adopted an "agile methodology" to introduce changes in processes and systems at a rapid pace. Instead of announcing a three-year project that may be difficult to digest, this respondent concentrates on implementing a series of security changes in "sprints" within much shorter timelines that show continuous value creation and ROI.

Third, cybersecurity should move from being a "no" to a "yes, and" organization. They need to be enablers of business, and as such should have a key place at the innovation table. To accomplish this, security professionals cannot be perceived as merely putting up barriers, but instead should be facilitating the drive toward digital banking, fintech, regtech, cloud adoption, digital identity, and other innovations to follow. This involves being part of the innovation councils at both the enterprise and LOB level, as well as having skills on the team to engineer next-generation solutions. CISOs need to be seen as striking the right balance between finding and asking for time for remediation vs. enabling the next frontier for the business.

TIPS FOR FSIs

- **Keep cyber initiatives digestible.** Deploy a rolling 18- to 24-month strategy with clear ownership for execution.
- **Establish an accountability model.** Ensure business, operations, and CIO teams understand their roles and have skin in the game.
- **Get ahead of the curve on innovation.** Build specific plans for cloud, fintech, regtech, and other cutting-edge developments.
- **Be problem-solvers, not roadblock builders.** Have a dedicated architecture and engineering team with technical skills to solve present and future problems.

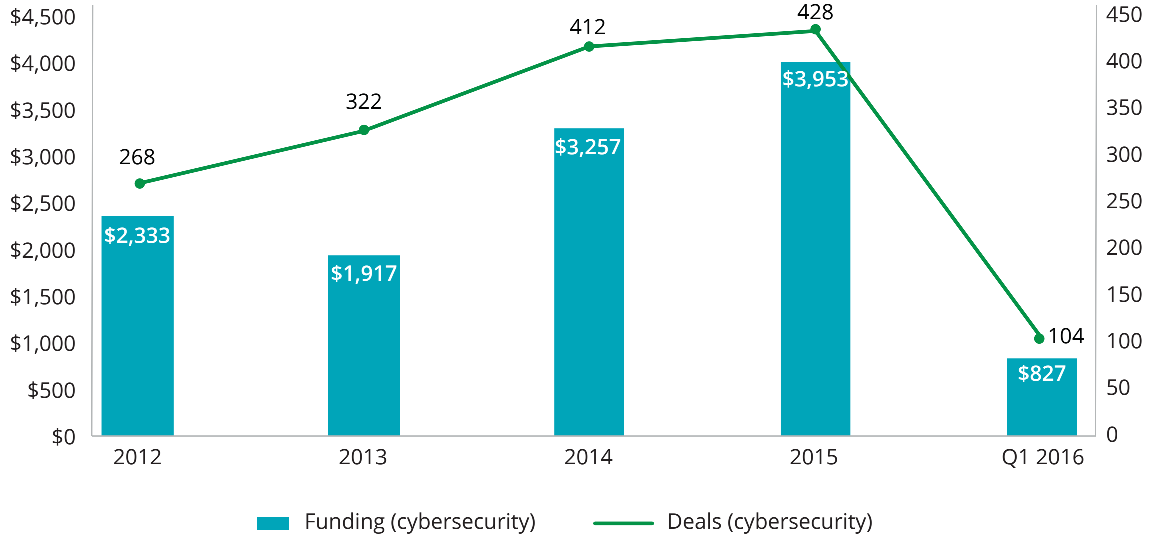
CISOs striving to innovate while struggling with new tech tools and organizational transformation

Where are FSIs now?

Necessity is the mother of invention, an axiom that certainly applies in the realm of cybersecurity, where increasingly sophisticated threat actors keep upping their games, forcing their targets to respond in kind with new defensive measures. As a hot market, cyber has seen a flood of investment dollars, with 1,430 deals struck between 2012 and 2015 to fund cybersecurity companies, totaling $11.46 billion[5] (see figure 4).

When it comes to security software, most respondents indicated they don't want to waste time or money "reinventing the wheel," especially since there is no guarantee they could come up with anything better on their own than what is already on the market. However, some collaborate with key vendors as strategic partners. In one example, an FSI and vendor worked together to innovate a new solution because, as the CISO explained, "There are times when what we want just doesn't seem to exist." Instead, they

Figure 4. Global cybersecurity funding ($M)



Source: CB Insights.

Graphic: Deloitte University Press | DUPress.com contracted with a vendor to create a new product that would meet their specifications, which they could pilot together. "If it works, they can sell it to the general market, but we have it first," he noted. A second respondent said his company is "mentoring" a start-up in "the deep, dark web space" to generate more innovative security options.

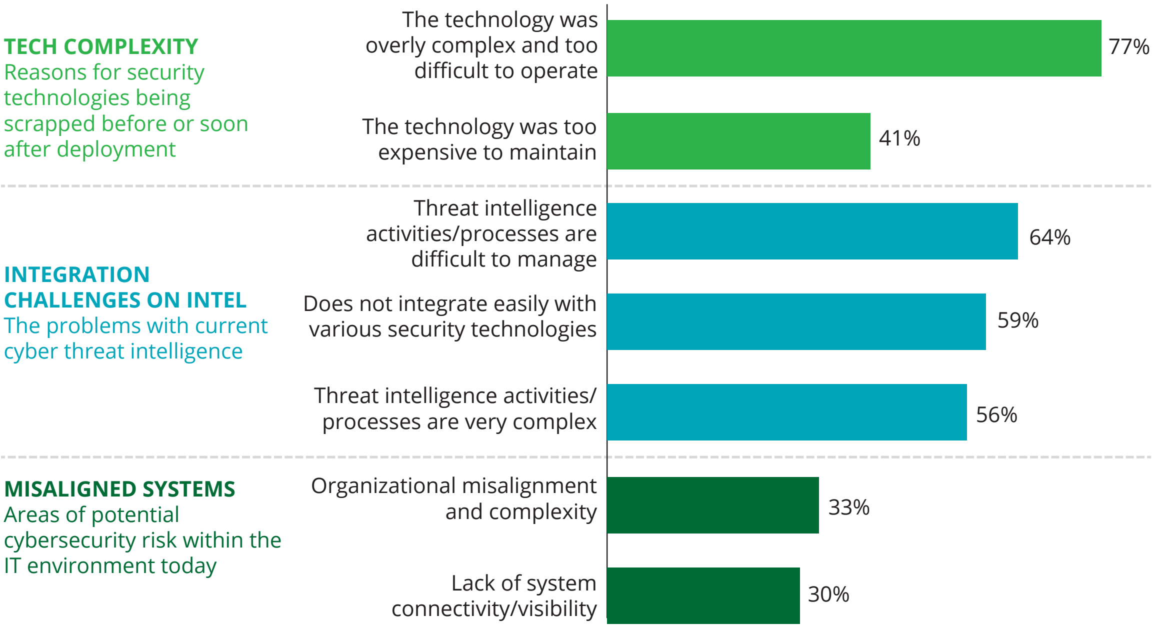
However, the fact that almost all of our respondents rely mainly on vendors for cybersecurity technology innovation doesn't mean the industry is satisfied with the products or services on the market today. Indeed, we found quite the contrary. CISOs frequently complained about what some called a "flood" of new cybersecurity solutions being pitched to them as start-ups proliferate. What's worse, many said vendors are pushing products that are either redundant to what they already have, or are simply nonessential to their core security efforts. This may portend a broader shakeout sometime soon in the security start-up space.

Amidst what one referred to as all the "noise" being generated by the steady stream of new offerings, many respondents said it is becoming increasingly difficult to decide which products they really need, as well as to distinguish who has a better mousetrap among competing vendors.

FSIs are also struggling to integrate multiple solutions into their legacy systems and reconcile them with other security products already installed (see figure 5).[6] Such integration efforts can cost many multiples more than the product itself. They also noted that rather than becoming fixated on the "next shiny object" hitting the market, getting basic foundational capabilities right (such as asset and configuration management, secure development practices, etc.) can go a long way to address core issues at many institutions.

Balance between external threat intelligence and internal, organizational intelligence was one particular area that generated a lot of dialogue. Many

Figure 5. Integration and complexity issues present remediation challenges for CISOs*



*Multiple industries, with financial services forming largest segment of the respondent base at 22%.

Sources: Lockheed Martin and Ponemon Institute, *Intelligence-driven cyber defense*, February 2015; Lockheed Martin and Ponemon Institute, *Risk and innovation in cybersecurity investments*, April 2015.

Graphic: Deloitte University Press | DUPress.com

felt that while some keep chasing intel from outside sources (described by one as "death by feeds"), there is not enough accountability and resources spent on operationalizing available threat intelligence and also being smart about internal intelligence—what one called "the organizational footprint."

Where might FSIs go from here?

Most FSIs conceded there are no easy answers to the dilemma of product proliferation. There has been a round of consolidation among cybersecurity vendors, with 133 merger and acquisition deals totaling $10 billion in 2015, according to 451 Research. That trend is likely to continue, as a 451 Research survey of tech investment bankers last December found that for the first time in five years, mobility was displaced by enterprise security as the top target of M&A spending for the year ahead.[7]

However, that trend is likely to be more than offset by ongoing launches of start-ups in the space, with 104 new companies financed in the first quarter of 2016 alone,[8] offering the promise of greater innovation from new players, but also perpetuating the fragmentation that is frustrating many CISOs. In the end, the need for more integrated solutions will remain high on the agendas of most we interviewed.

Some CISOs are taking field trips, traveling to Silicon Valley and other creative hubs to stimulate their thinking on cybersecurity innovation. At least one FSI has set up an innovation lab in Israel, while another made a "pilgrimage" there, which he said can be described as "the Promised Land" for risk management, thanks to its ecosystem of cyber start-ups and a skilled talent pool drawn from high-tech military intelligence operations. Taking this one step further, companies are also looking to accelerate their innovation activities by engaging with a lab as a service/engineering partner. This could help FSIs stay ahead of the innovation curve, but also focus their own organizational resources on solutions that matter.

When it comes to specific cyber innovations, cloud technology generated the most buzz among those we interviewed. Some CISOs hope cloud solutions could be a cybersecurity panacea, believing it is unlikely their company could do a better job protecting data and systems on its own. On the other extreme were those who worry that the cloud, whatever its business advantages, might create new cyber vulnerabilities such as concentration risk, issues during incident response, and other problems.

The rest fell somewhere in between hope and fear. However, one CISO emphasized that regardless of the path a company chooses, the primary security burden is still on the FSI, "even if you forklift all your existing applications to the cloud." He explained that the cloud does not relieve companies of responsibility for putting basic security processes in place, as well as keeping them well-maintained and regularly upgraded. Some companies have or may choose to build their own private clouds to retain direct control over cybersecurity. But the question is whether that fallback option would be less expensive, more agile, or any more reliable from a security standpoint than the risk management protocols of a third-party cloud provider.

Another area where we may soon see innovation is the adaptation of blockchain technology to enhance cyber risk management. In addition

Looking at the bigger picture, most respondents warned that innovation in tech tools alone cannot provide adequate cybersecurity.

to protecting transactions and facilitating counterparty validation, the shared yet secure use of blockchain ledgers may be leveraged to mitigate traditional cyber problems. It's all about ensuring that any changes to the integrity of an FSI's important assets can be detected, with blockchain serving as an enabler providing a deeper level of situational awareness.

Let's take endpoint detection as an example. Imagine having a cryptographic key for your workstation that is then subsequently monitored. This means all your system/user processes, memory, etc., could conceivably be tracked by the blockchain. Thus, any deviations, such as newly installed malware running on a workstation, could be detected and used as an additional piece of intelligence. The information that would be extracted from this event could be infused into traditional security devices such as firewalls and intrusion detection systems.

Still, looking at the bigger picture, most respondents warned that innovation in tech tools alone cannot provide adequate cybersecurity. Indeed, the need to innovate extends beyond technology into how an FSI might transform its security maturity.

One emerging concept, borrowed from the federal government and law enforcement agencies, is to create a cybersecurity fusion center, integrating disparate teams from different parts of the organization. These teams have very diverse skill sets, from intelligence, forensics, operations, physical security, fraud, data science, and other related areas. Such teams are designed to create around-the-clock situational awareness, rapidly share intelligence across the organization, and break down organizational barriers to take action, as well as act as a "hub" when dealing with crises. Fusion center teams can also work across the ecosystem (partners, vendors, customers, etc.) to extend situational awareness.

Another organizational discipline that has taken hold is to establish cyber risk managers in each LOB, who coordinate their efforts through the company's CISO. This way, cybersecurity has boots on the ground across the organization, and can more effectively communicate information both ways—identifying business needs for risk management from the front lines, while pushing out loss control practices from the security command center. One company reported an 86 percent reduction in what it called "critical risks" in one calendar year because business leaders started becoming part of the solution in this fashion.

Cyber war-gaming, and in some cases, red-teaming, has also emerged as an organizational innovation to create a battle rhythm and muscle memory for dealing with cyber issues. Many firms conduct multiple exercises (four to eight) annually, while some larger ones conduct 20 or more a year, covering the gamut from board and C-suite participation, to LOB-specific exercises, to others focused on certain scenarios. War-gaming is being extended to customers, business partners, vendors, and other third parties to allow for shared preparedness and coordinated crisis management during a cyberattack.

These war-games are multidisciplinary and involve not only technical cyber teams but broader participation among representatives from business, IT, communications, legal, and other departments. They answer questions such as: What happens if you get a call from law enforcement about a cyber breach? Or from the media? Do you have privacy notification firms on retainer? Have you contracted with forensic firms? Is outside counsel on call if the worst-case scenario is realized? "You don't want to have to think about these things while you're having a crisis," one CISO warned.

Better leveraging of data and analytics was also cited as a major source of potential innovation by those interviewed. One company is exploring ways to utilize big data technology that's already available on the customer side of the business to improve cybersecurity as well. It has data scientists helping IT security assess threat scenarios, evaluate available data points, and develop cyber risk models.

Another respondent cited the importance of analytics when it comes to detecting and thwarting non-malware-based compromises. Behavioral analyses are crucial in determining whether a user or system is behaving the same as the day, week, month, or year before. "The analytics pieces have the ability to open up visibility into the sort of softer things that you simply can't write a rule about," this CISO said, adding that the only way to really deal with that effectively is "statistically and probabilistically."

Another CISO said his organization is looking to develop "cyber warriors" who would be trained to be better prepared to anticipate potential breaches by using advanced data analytics. Their mission would go beyond looking for indicators; their marching orders would be to get ahead of the threat actors and anticipate attacks rather than remediate after the fact. They would accomplish this, in part, by injecting themselves into the ecosystem and using counterintelligence techniques to see where hackers and disruptors are trying to operate.

A word of caution, however. When dealing with analytics, it's usually a good practice to start off small. Rather than collect sweeping sets of data from the entire organization and then figure out what to make of it all, CISOs need to do more critical thinking at the front end to determine exactly what they want to accomplish and which data they'll need to fulfill their goals. It was suggested they follow the example set by those using analytics to generate machine learning in basic fraud detection and anti-money laundering efforts, where the problems and solutions are tightly defined.

TIPS FOR FSIs

- **Focus on product integration and lifecycle management.** Avoid redundancy and understand integration challenges. Don't introduce a product if you don't have the talent to support it.
- **Innovate process and structure, not just technology.** Consider the 10 dimensions of innovation and apply them to security, including non-tech elements such as business model, channel, and core processes.[9]
- **Learn from the business side.** Leverage analytics lessons and expertise to innovate for cyber.
- **Collaborate at all levels.** War-gaming, intelligence sharing, and fusion centers generate threat awareness and insights across the enterprise.

Cybersecurity starving for "triple-threat" talent

Where are FSIs now?

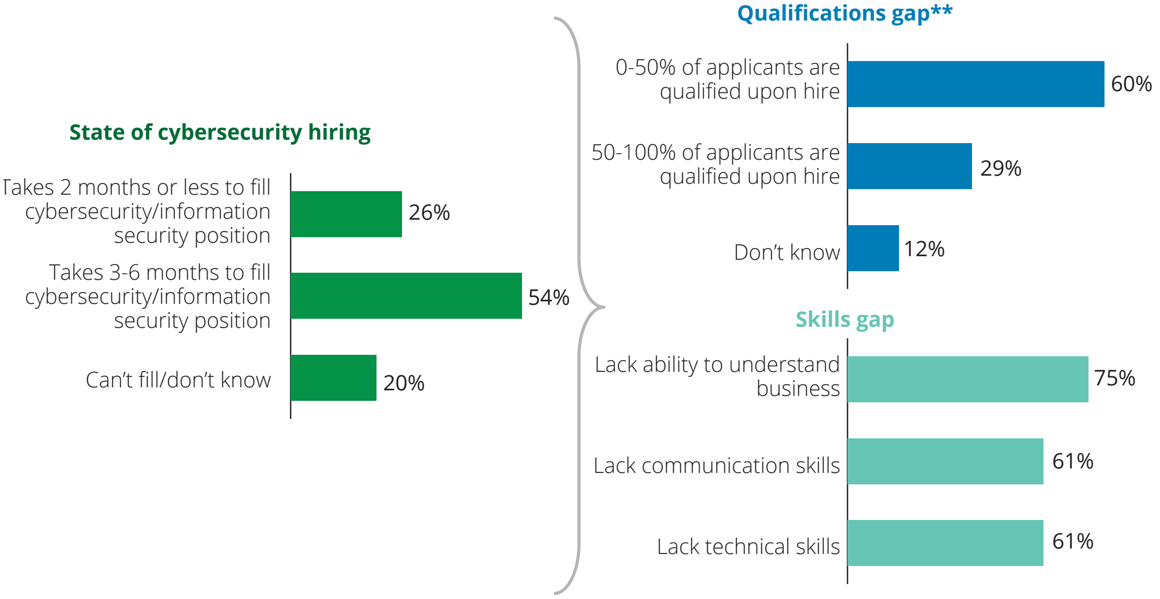
While funding for cybersecurity may be abundant, a survey by ISACA found that qualified talent is in extremely short supply (see figure 6),[10] so it's not surprising that many of those we spoke with cited the inability to bridge the talent gap as their top challenge. The resulting lack of ample in-house expertise makes it difficult for companies to innovate, deploy new security technologies, and launch intelligence-driven cyber defenses (see figure 7).[11]

Our interviewees certainly were in agreement with these findings. Most were vehement that if you don't have the right people with the necessary skill sets at your disposal to formulate and execute strategies for security, vigilance, and resilience, it won't matter what solutions a company buys or builds because projects won't get the level of execution they need.

One stated that, "There are many pretenders, but not enough real talent." While a number of new university cyber risk management programs have been launched of late, it will likely take five years or more before businesses start seeing the full benefit of that investment, leaving a significant, lingering talent gap to fill in the interim.

Complicating matters is that many companies are looking for "triple threats"–not merely data

Figure 6: Talent in short supply*

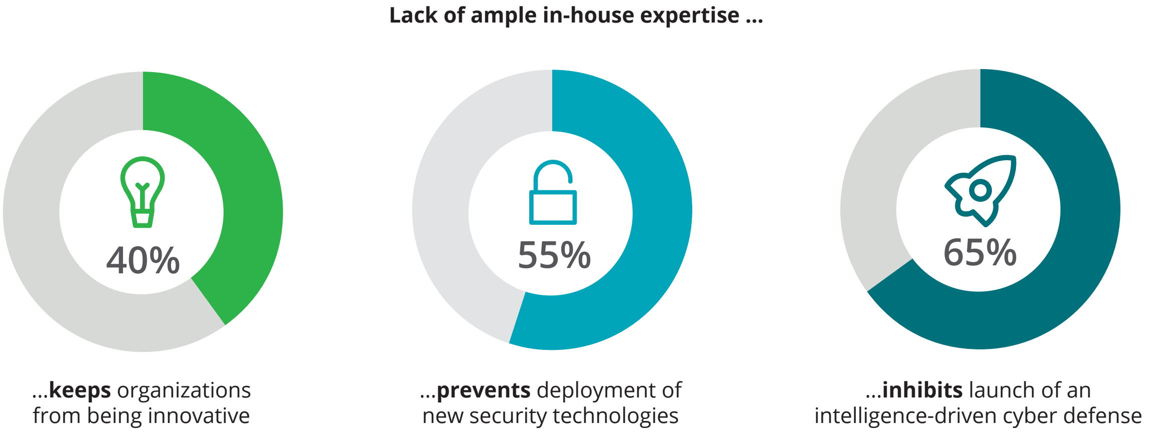


*Multiple industries, with financial services forming largest segment of the respondent base.
**Percentages do not add up to 100% due to rounding.

Source: *State of Cybersecurity: Implications for 2016*, ISACA and RSA Conference Survey, March 2016.

Graphic: Deloitte University Press | DUPress.com

Figure 7. Impact of talent gap*



*Multiple industries, with financial services forming largest segment of the respondent base.

Sources: Lockheed Martin and Ponemon Institute, *Intelligence-driven cyber defense*, February 2015; Lockheed Martin and Ponemon Institute, *Risk and innovation in cybersecurity investments*, April 2015.

Graphic: Deloitte University Press | DUPress.com

scientists and security technology specialists, but also those who understand strategic planning as well as how to integrate cyber risk management without unreasonably inhibiting business development or undermining customer experience. Most CISOs also cited a need for communication as well as problem-solving skills. Changing talent needs and expectations are being driven by the transition of cybersecurity from an IT-centric, purely technical facilitator to a business risk function. One respondent quipped, “People like this don’t grow on trees.”

Respondents also questioned the lack of a security services strategy that exacerbates the talent issue. Some organizations believe that they have to build all security services internally, and very soon will find it extremely difficult to hire, train, grow, and retain talent across all disciplines. Some organizations, as part of their overall strategy, have undertaken a conscious and often painful debate about which services they should retain internally and which they should cosource or outsource while managing the risks. Crowdsourcing is another phenomenon that FSIs are starting to test-drive, with some start-ups using that as a model to identify skilled resources. While interesting, crowdsourcing has also raised a number of questions about the inherent risks of giving critical tasks to an unknown person or someone not vetted by the company.

Exacerbating the problem is that companies frequently complained about turnover. In that regard, FSIs have some blame to share, because many poach talent from peer organizations, prompting a continuous movement of people among the institutions. One CISO estimated his department spends 20 percent of the time seeking the right talent, particularly to back-fill those moving on to greener pastures. Many said they had lost a significant number of key people to vendors, fueled in part by the proliferation of cybersecurity start-ups. A few pointed out their vendors and service providers are having a hard time holding onto people as well, which could upset the continuity of projects. This calls attention to the need to assess bench strength when engaging an outside firm for products or advice.

Where might FSIs go from here?

So, what solutions are available to companies to win the war for talent? A number of those we interviewed emphasized the importance of broadening talent searches beyond financial services, an industry that one major player characterized as very insular in its thinking and approaches. When it comes to recruitment, he pointed out, "There's a whole world of talent out there that we're failing to reach out to." Recruiting talent into financial services from other fields—such as the military, government intelligence agencies, or nonfinancial industries—can therefore be quite helpful not only in deepening the prospect pool, but also in bringing a fresh perspective to tackle the industry's challenges.

However, the time and difficulty in getting some non-FSI talent up to speed on the particular needs and challenges of financial services should not be underestimated, meaning a rigorous process is necessary to onboard outsiders quickly and effectively. This could be accomplished internally or with outside help.

However, the advantages of importing new talent doesn't mean FSIs should ignore the growth potential of current employees. Indeed, many respondents suggested companies follow a two-pronged strategy by simultaneously creating a farm system to develop in-house talent. One company found plenty of internal prospects for cyber risk management positions working in other tech-related departments. While such individuals may not have direct experience in security, they are more likely to understand how the industry and their particular company functions both operationally and technologically, making them prime candidates for a transfer and retraining. Others have created strategic relationships with select campuses to identify and grow new talent.

One CISO estimated his department spends 20 percent of the time seeking the right talent, particularly to back fill those moving on to greener pastures.

Mixing and matching could be another solution. A number of companies have started sharing learnings and resources across cyber, physical security, fraud prevention, anti-money laundering, and other related departments. While there may be a culture clash at first, eventually those employing this approach reported lots of synergy and good ideas emerging as disparate parties feed off one another's varied experiences. One example was a firm looking to bolster its predictive capabilities on cyber risk by leveraging its longstanding financial fraud unit, which already had experience using analytics to spot suspicious behavior.

It also might be wise for companies to stop thinking about hiring elusive "triple threats" and instead focus on building multidisciplinary teams with complementary skill sets and expertise. This might help cover the breadth and depth of risks these companies face as cybersecurity becomes increasingly aligned with business risk. Assembling such teams could be accomplished internally, or by leveraging specialists from outside providers as needed. A number of those we interviewed said they use third parties to mitigate recruiting difficulties and talent shortages, in effect "renting capabilities," as one CISO described the practice. Resource shortages may prompt FSIs to rethink their operating models, in terms of which capabilities need to be retained in house vs. those that might be supplemented by outside service providers.

It is also important to start putting security responsibility where it belongs. For example, application development teams should be trained to build security requirements into their work, and be held as accountable for secure code as much as they are for functional and performance requirements. In another instance, one CISO began sharing with senior management the names of the worst offenders among employees repeatedly failing phishing tests, a development which soon started driving improved security behavior.

Meanwhile, FSIs might consider launching a collective industry-wide talent development and recruitment campaign. Such a collaborative approach—perhaps backed with scholarship funding for technology students in college or graduate school, or recruitment drives to educate non-traditional candidates with critical thinking and analytical skills from the arts or humanities—could help bolster the ranks of those choosing a career in FSI-related cyber risk management.

TIPS FOR FSIs

- **Lead the charge in creating a cyber talent model.** Establish an expectations framework in concert with industry associations and government.
- **Define a focused human capital strategy.** Partner with your talent team to develop next generation "cyber ninjas." Recruit inside and outside the company and industry.
- **Rotate talent to expand capabilities.** Draw expertise from tech, business, fraud, anti-money-laundering, and physical security teams.
- **Focus on core cyber functions.** Consider cosourcing or outsourcing the rest.

Risk metrics remain a Tower of Babel as reporting responsibilities overwhelm CISOs

Where are FSIs now?

Former New York City Mayor Ed Koch was famous for seeking feedback from constituents while riding the subways or standing on street corners. His signature slogan during such jaunts among the masses was, “How’m I doing?” He usually got an earful.

Cyber risk executives are in much the same position, racing to keep up with mounting exposures and responsibilities while struggling to meet the oversight demands of a growing number of internal and external stakeholders. Making these challenges more difficult to overcome is a general dissatisfaction among CISOs we interviewed with the metrics currently employed to measure their progress, as well as a lack of standardization in terms of what they have to report to all those looking over their shoulders.

One respondent summed up the prevailing sentiment in calling for cyber risk metrics that are “easy to understand, common across the industry, and automatable, but that’s simply not the case today.” Many indicated they are operating in a vacuum, without any industry-wide benchmarks against which to measure their organization’s cybersecurity maturity level. Almost all cited considerable hardship in dealing with different, yet often redundant reporting requirements.

This latter point is particularly significant, as many interviewees complained that they are spending as much as half their time explaining what they’re doing—to regulators and auditors, as well as their CIOs, senior management teams, and board members—rather than actually practicing cyber risk management. It’s come to the point for many where reporting duties are beginning to hinder operational efficiency. One cited a severe case of “audit fatigue,” while another said a “cottage industry” has arisen in their department to respond to reporting requests. Yet another wearily characterized the “constant cycle of explanation” they must endure as “very déjà vu.”

A big part of this problem is what one respondent described as “regulatory disharmonization,” expressing concern that the lack of standardization in reporting expectations is “getting so out of hand it’s creating risks rather than preventing them.”

US Senator Dean Heller of Nevada spotlighted this issue in a letter to US Treasury Secretary Jacob Lew and Federal Reserve System Governor Daniel Tarullo on March 4, 2016. Heller, a member of the Senate Banking, Housing, and Urban Affairs Committee, wrote, “Much better coordination is

> Many indicated they are operating in a vacuum, without any industry-wide benchmarks against which to measure their organization’s cyber-security maturity level.

needed among the various financial regulators to ensure a consistent cybersecurity risk management approach that does not waste precious time or valuable resources that could be used in the ongoing defense against cybercriminals." He asked the Treasury and Fed what they could do in coordination with other federal oversight bodies to avoid "unnecessary duplication" in reporting requirements.[12]

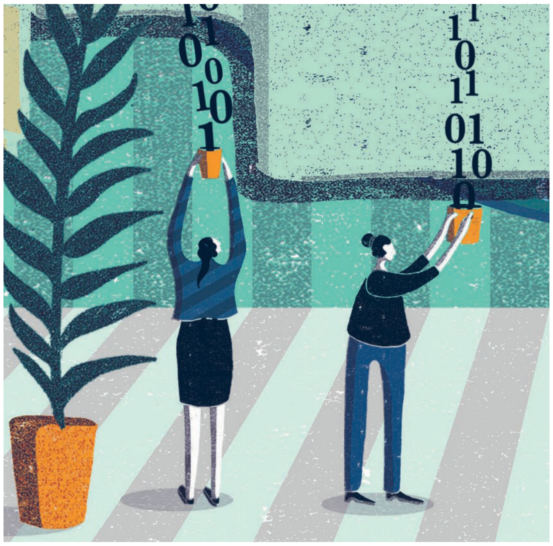
Adding fuel to the fire is the fact that metrics are becoming more than just a risk management or compliance exercise. One executive we spoke with said his team is often pulled into request-for-proposal preparations because the effectiveness of his organization's cyber program has become a key factor for commercial clients in deciding where to place their business.

Where might FSIs go from here?

Given that measuring the impact of cybersecurity is "still more art than science," as one of our respondents put it, how might FSIs get a better handle on the state of cyber risk management at their companies? How might well-intentioned yet increasingly burdensome reporting demands become more manageable and productive?

In terms of settling on the most impactful metrics, some respondents suggested that instead of focusing just on the number of attacks or intrusions, the key measure should be a company's response time and effectiveness in containing threats. How soon are intrusions detected? How quickly does a company respond? How seriously are systems compromised, and how much damage is done? How long does recovery take? How is the impact on operations minimized?

Along those lines, a holistic view is much more relevant, with metrics based not on whether individual controls are effective in isolation, but whether a layered series of controls do the job in the aggregate. For example, when dealing with malware, companies may be less concerned about the infection of an individual computer than whether there's any wider adverse impact. Was the intruder able to steal any valuable information or do any damage to broader systems from that one compromised device? Did the intrusion spread beyond that user, department, or office?



One CISO goes this route by emphasizing "dwell time," measuring how long intruders linger once they penetrate a company's system, with the goal being to limit their ability to move laterally and do serious damage once they're inside. If detection and mitigation systems quickly respond and isolate an intrusion before any significant loss is sustained or disruption accomplished, that should be considered a win, this respondent concluded. At least one company even chooses to let intruders stay for a while to monitor them and try to learn what they are after before blocking them and kicking them out of their system.

Qualitative analysis may also help communicate the effectiveness of cyber risk management programs, a number of respondents noted. One FSI replaced its purely quantitative cyber risk scorecard with scenario assessments, examining individual operations from an enterprise risk tolerance perspective. How prepared is the company to counter a particular threat? How close or far is it from being ready? What does it need to do to be ready to offset each risk?

Another respondent suggested that storytelling is an important component in demonstrating the value of cybersecurity in real terms, noting that his company provides narratives in its reports on risks averted, disruptions avoided, and money saved to show tangible benefits. “If we can get a great success story each week, that’s a win,” he said.

Such an approach can be particularly effective when presenting reports to board members. One of those interviewed said boards generally have three bottom-line qualitative questions: Are you able to identify cyber risk and get the enterprise behind managing that exposure? Can you then prioritize what’s most important? Do you have the resources you need to get the job done?

In terms of standardization, respondents indicated that they crave leadership at both the industry level as well as by the government to drive dialogues. CISOs are seeking certainty in assessing and reporting their status. Along those lines, it would be ideal to have a widely accepted “cyber risk balance sheet” at their disposal. Cybersecurity frameworks have been developed and are starting to gain wider adoption, but as one respondent observed, “Everyone is modifying them for their own purposes. There are very different views of what ‘good’ looks like.” These frameworks need to continue evolving, offering additional guidance around the metrics component and what optimal reporting should involve.

CISOs will likely need outside help and broad cooperation to achieve the desired state of measurement and reporting nirvana. In accounting, regulators drive standardization. Therefore, not having a centralized body—either public or private—to set the bar for cyber risks is perhaps the main industry-wide problem that needs to be overcome.

Those we interviewed agreed that standardization would go a long way toward making the reporting process not only more efficient and cost-effective, but more impactful as well. Therefore, getting everyone with skin in the cyber risk management game to rally behind standards could be a key goal for the industry going forward.

TIPS FOR FSIs

- **Implement a formal communication plan.** Tailor to audiences using the same core message.
- **Coalesce reporting around the top 20 metrics.** Among hundreds of data points that can be collected, build consensus within the organization on what matters most.
- **Integrate data into an overarching narrative.** Include qualitative stories with statistics; provide context and real-life results to engage stakeholders.
- **Automate whenever possible.** Keep moving toward real-time risk sensing.
- **Implement a rapid reaction force.** Stay on top of industry events and how your company is responding.

CISOs need help connecting the dots with intelligence sharing and analytics

Where are FSIs now?

In 1776, Benjamin Franklin told his fellow members of Congress at the signing of the US Declaration of Independence, "We must all hang together, or assuredly we shall all hang separately."[13] That sage piece of advice should resonate with cyber risk managers because they, too, face a common enemy. Those we interviewed seemed to agree that information sharing among trusted parties is critical. Such cooperation helps alert potential targets about emerging threats, and forces attackers to continue coming up with new ploys and techniques.

Yet even though there are a number of formal and informal networks in place, intelligence sharing still leaves much to be desired for a variety of reasons. Many respondents cited conflicting local and international regulatory boundaries as a significant obstacle. Others lamented a lack of information specific to FSIs in general and their own industry sector in particular. Some noted there are legal and policy barriers within their environment hindering the free flow of information.

But the biggest complaint was the inability to make sense of all that's shared so companies can better anticipate and head off potential cyberattacks. One CISO said the industry is still in its "infancy" in this regard, observing, "Our raw mathematical capability is outpacing what we can actually do with all the data we're collecting."

High on the wish list of our respondents was a way to automate threat assessment to help their human analysts "connect the dots" so they sense a threat quicker and can respond more proactively. One CISO observed that while there are "tons" of providers for threat intelligence, technology and processes are needed to make such information more consumable and actionable by either humans or machines—described by this individual as the "secret sauce."

Where might FSIs go from here?

There is no shortage of opportunities to swap cyber war stories from the front lines. Beyond attending conferences and other gatherings hosted by cyber risk organizations, industry associations, and government agencies, many of those we interviewed found the most value from the informal networks they've built over the years. One respondent said he depended upon "a circle of trust": colleagues from other firms, both inside and outside financial services, whom he can turn to in a crisis and use as a sounding board. Some organizations are considering extending that circle to their strategic clients as well as vendors and other partners in order to share intelligence.

Yet despite good intentions, information sharing can be problematic given the potential liability and logistical hurdles that often must be cleared. Many said they are still not comfortable pooling information, despite new legislation facilitating such collaboration, because they are unclear about what they can share legally. And while greater clarity from lawmakers on this front would be welcome, intelligence sharing will likely remain problematic if only because, as one respondent put it, “You can’t legislate trust. It’s going to take years to develop.”

Information overload becomes an even bigger issue when you consider that FSIs are also purchasing intelligence from a number of private vendors, with mixed results. One particular complaint was the amount of generic data being supplied, as opposed to intelligence specific to financial services, or even to one specific sector or company–given that threat actors are specializing down to the individual firm level. Others lament the necessity of having to piece together data from a wide variety of sources to create relevant, useful information.

The biggest challenge respondents cited in this area is improving their ability to leverage the data collected from a wide variety of sources to produce predictive analytics that more quickly expose and head off looming threats. Many expressed a desire to shift emphasis from volume-focused intelligence (trying to get more and more data) to action-focused. (How can they maximize the use of all this information?)

While there are a number of risk assessment tools and systems on the market, many respondents called for greater automation of threat intelligence in a rules-based system that filters, integrates, and analyzes available data without human intervention. Such capabilities today are “super immature right now,” according to one interviewee, who said, “Automation could potentially be game changing if we can get a groundswell on that.”

Respondents also called for organizations to strike more of a balance between dependence on external vs. internal intelligence, with the latter focused on improving situational awareness and monitoring anomalous user behavior. To that end, the use of big data analytics and machine learning to solve cyber problems generated much discussion and debate. Some organizations said they are struggling to justify ROI or prioritize such efforts, described by one respondent as “a hammer looking for a nail.” Others continue to invest through targeted pilots.

TIPS FOR FSIs

- **Form “circles of trust” to bolster intelligence sharing.** Reach out to peers, partners, clients, and vendors.
- **Turbocharge human analysis with automation.** Pilot threat intelligence management platforms.
- **Balance external and internal intelligence.** Improve situational awareness with big data analytics and machine learning.
- **Promote regular threat briefings.** Package with success stories for target audiences.

Looking ahead: No rest for the weary in cyber risk management

FOR those on the front lines in cyber risk management, the good news is that senior leadership and board members are well aware of the seriousness of the exposures their companies face and have been very supportive of efforts to make FSIs more secure, vigilant, and resilient. Indeed, the companies we interviewed appear to be willing to invest whatever it takes to enhance cyber risk management personnel, processes, and technology in the short term and long term.

At the same time, however, many FSIs continue to feel underprepared to detect and ward off the ever-evolving threat of massive financial fraud or data loss, and are increasingly worried about destructive attacks or coordinated assaults against the financial ecosystem.

Part of the problem is that FSIs are still often flying blind, grappling with the particulars of how to measure and report their progress in containing cyber risk, as well as determine how they stack up against their peers. They are also having trouble deciding how much information they are willing and able to share with others facing a common enemy. Last but not least, figuring out how they can most effectively leverage the data they collect from a wide variety of sources to produce reliable, predictable, and actionable intelligence remains a work in progress.

Many of those we interviewed expressed frustration about getting a handle on this elusive exposure. “We sent a man to the moon and back, so why can’t we solve this?” lamented one respondent. The answer may be that cyber risk management is a never-ending game of cat and mouse. As soon as one security gap is closed, another breach is attempted through a different system, application, or technique. As one respondent put it, “The reality is, cybersecurity risk management is an ongoing journey, never a destination.” Therefore, CISOs will need to be continuously on guard and innovative to keep up, let alone stay ahead of the bad guys trying to break into their systems 24/7.

To accomplish this, risk managers need to not only hit moving targets as they arise; they need to do a better job proactively probing for weaknesses in their environments. They also have to manage expectations. While zero tolerance is an unrealistic goal when it comes to protecting their institutions, containment of the damage is doable. For example, one respondent echoed a number of his colleagues when he spoke about looking to “compartmentalize” his network to “restrict the blast radius of an attack.”

They also must improve their talent development and recruitment efforts. Attracting, training, and retaining the right people, as well as managing the complexities of the job, takes far greater leadership and innovative thinking than it used to.

Beyond the CISO’s immediate circle, marshalling people power, not just technology solutions, is a big part of the containment effort. Whereas FSIs may have covered most of the bases in terms of

> As one respondent put it, “The reality is, cybersecurity risk management is an ongoing journey, never a destination.”

raising awareness of cyber risks, the next frontier is to influence actual behavior. Are stakeholders acting on their awareness, or merely "checking the box" when alerted about potential cyber vulnerabilities?

Still, despite all their best efforts, most FSIs are likely to see their systems breached or compromised at some point, so recovery and resiliency are two critical back-end considerations. A number of those we spoke with are running more than just table-top exercises or war-gaming, where the consequences of a cyberattack are theoretically handled in a laboratory setting. Some are running live exercises so they can keep their businesses up and running the old-school way after a serious event. One went so far as to note, "We are preparing to recover our services from bare metal if necessary."

In the end, CISOs cannot defend their organizations alone. They need collaboration, cooperation, as well as shared responsibility and accountability to permeate a cybersecurity mentality across the entire enterprise.

But CISOs can and should be leading the charge to spread the word about what's at stake for everyone involved, and what must be done to counter and contain the threat. Their role in the organization should be enhanced to help FSIs meet this existential challenge. With greater power will come greater responsibility, but the elevation of CISOs may be necessary to make cybersecurity, vigilance, and resilience considerations second nature in every facet of an FSI's business operation. Only then can the risk management efforts of informed employees, vendors, partners, and customers be coordinated to serve as effective antibodies against those threatening to do their companies harm.

ENDNOTES

1. Ponemon Institute (sponsored by Hewlett Packard Enterprise), *2015 cost of cyber crime study (United States)*, October 2015, http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states.
2. Deloitte Touche Tohmatsu Ltd., *Global risk management survey*, ninth edition, May 2015, http://www2.deloitte.com/ru/en/pages/financial-services/articles/9th-global-risk-management-survey.html.
3. Ibid.
4. Verizon, *Data breach investigations report (financial services industry reports)*, April 2016 and October 2012, respectively, http://www.verizonenterprise.com/verizon-insights-lab/dbir/.
5. Based on statistics provided by CB Insights.
6. Ponemon Institute (sponsored by Lockheed Martin), *Intelligence driven cyber defense*, February 2015, http://cyber.lockheedmartin.com/intelligence-driven-cyber-defense-survey-results, Ponemon Institute (sponsored by Lockheed Martin), *Risk and innovation in cybersecurity investments*, April 2015.
7. 451 Research, “451 Research identifies nearly 300 M&A and IPO candidates in its annual 2016 tech M&A outlook,” February 26, 2015, https://451research.com/images/Marketing/press_releases/02.25.16_MA_Out-ook_2016_PR_Final.pdf.
8. Based on statistics provided by CB Insights.
9. Larry Keeley et al., *Ten Types of Innovation: The Discipline of Building Breakthroughs* (New York: Wiley, 2013).
10. ISACA and RSA conference survey, “State of cybersecurity: Implications for 2016,” March 2016, ©2016 ISACA. All rights reserved. Used by permission.
11. Ponemon Institute, *Intelligence driven cyber defense* and *Risk and innovation in cybersecurity investments*.
12. Credit Union National Association, *CUNA News*, “Sen. seeks FSOC-FFIEC plan for coordinating cybersecurity exams,” March 8, 2016.
13. The Quotable Franklin, UShistory.org, accessed April 7, 2016, http://www.ushistory.org/franklin/quotable/singlehtml.htm.

ABOUT THE AUTHOR

SAM FRIEDMAN

Sam Friedman is the insurance research leader at the Deloitte Center for Financial Services in New York. He joined Deloitte in 2010 after three decades as a business journalist, most prominently as the longtime editor-in-chief of *National Underwriter*. At Deloitte, his research has explored consumer behavior and preferences in auto, home, life, annuities, and small-business insurance. Additional studies have examined how auto carriers can leverage telematics to improve underwriting and marketing for usage-based insurance, what the financial services industry might do to more effectively help consumers achieve retirement security, as well as how insurers might apply strategic risk management concepts to avoid disruption.

CONTACTS

Industry leadership

Kenny M. Smith
Vice Chairman
US Financial Services Industry Leader
Deloitte LLP
+1 415 783 6148
kesmith@deloitte.com

Deloitte Center for Financial Services

Jim Eckenrode
Managing Director
Deloitte Center for Financial Services
Deloitte Services LP
+1 617 585 4877
jeckenrode@deloitte.com

Sam Friedman
Insurance Research Leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Cyber risk management subject matter specialists who led this project

Vikram Bhat
Financial Services Cyber Risk Services Leader
Advisory Principal
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

Julie Bernard
Advisory Principal
Deloitte & Touche LLP
+1 714 436 7350
juliebernard@deloitte.com

Christopher Stevenson
Managing Director
Deloitte & Touche LLP
+1 201 499 0584
chstevenson@deloitte.com

ACKNOWLEDGEMENTS

The Center wishes to thank the CISOs and other cyber risk management professionals at financial services institutions who agreed to share their experiences and insights for this report.

The Center would also like to thank the following Deloitte client service cybersecurity professionals for their support and contributions:

- **Taryn Aguas**, advisory principal, Deloitte & Touche LLP
- **Sunny Aziz**, advisory principal, Deloitte & Touche LLP
- **Isaac Kohn**, senior manager, Deloitte & Touche LLP
- **Guarav Kumar**, advisory principal, Deloitte & Touche LLP
- **Bruno Melo,** partner, Deloitte Canada LLP
- **Emily Mossburg**, advisory principal, Deloitte & Touche LLP
- **Kieran Norton**, advisory principal, Deloitte & Touche LLP
- **Ash Raghavan**, advisory principal, Deloitte & Touche LLP
- **Adam Thomas**, advisory principal, Deloitte & Touche LLP

The Center would also like to thank the following Deloitte professionals for their support and contributions:

- **Michelle Canaan**, manager, Deloitte Center for Financial Services, Deloitte Services LP
- **Michelle Chodosh**, marketing manager, Deloitte Center for Financial Services, Deloitte Services LP
- **Sallie Doerfler**, senior market research analyst, Deloitte Center for Financial Services, Deloitte Services LP
- **Karen Edelman**, manager, US Eminence, Deloitte Services LP
- **Junko Kaji**, senior manager, US Eminence, Deloitte Services LP
- **Lisa DeGreif Lauterbach**, Financial Services Industry marketing leader, Deloitte Services LP
- **Seth Raskin**, manager, Deloitte Services LP
- **Lincy Therattil**, manager, Deloitte Center for Financial Services, Deloitte Services India Pvt. Ltd.

Deloitte.
University Press

Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication
This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Cover illustration by Lucy Cartwright.