Deloitte.
Insights

FINANCIAL SERVICES | Information Sharing and Analysis Center

The state of cybersecurity at financial institutions

There's no "one size fits all" approach

A report by the Deloitte Center for Financial Services and the Financial Services Information Sharing and Analysis Center (FS-ISAC)

Deloitte offers a complete portfolio of services to help complex organizations establish their cyber risk appetite, design and implement Secure.Vigilant.Resilient.™ programs, and assist in the ongoing management, maintenance, and adaptation of their programs as the business, compliance, and threat environments change.

CONTENTS

CISOs strive to upgrade cybersecurity

How do you measure what "good" looks like when it comes to cybersecurity at financial services companies?

THE answer may be difficult to determine in the midst of a constantly changing threat landscape, and at a time when shifting business priorities and exponential technology forces are changing how many organizations approach management of cyber risks. In dealing with these challenges, chief information security officers (CISOs) often face a number of difficult questions:

- Does the operating model (centralized vs. decentralized) matter?
- Which factors determine the role of CISOs in terms of reporting relationships and influence within their companies?
- What role does the innovation agenda play in deciding how much of the cyber risk budget could be used for transformative vs. operational investments?
- Is there an "efficiency ratio" that can be applied to cyber risk management functions?
- Is there an empirical way to compare one financial institution's cyber risk management program to another?

We surveyed CISOs from 51 companies about how they are discharging their responsibilities in protecting the digital fortresses at banks, investment management firms, insurance companies, and other financial services institutions (FSIs). The results provide a preliminary snapshot of how many FSIs may go about handling cybersecurity, while generating intriguing insights that warrant further exploration.

Overall, we found organizations working within a broad spectrum of cybersecurity strategies, structures, and budget priorities. Our findings suggest that clear differences exist within the industry based on company size, maturity level, and even ownership structure.

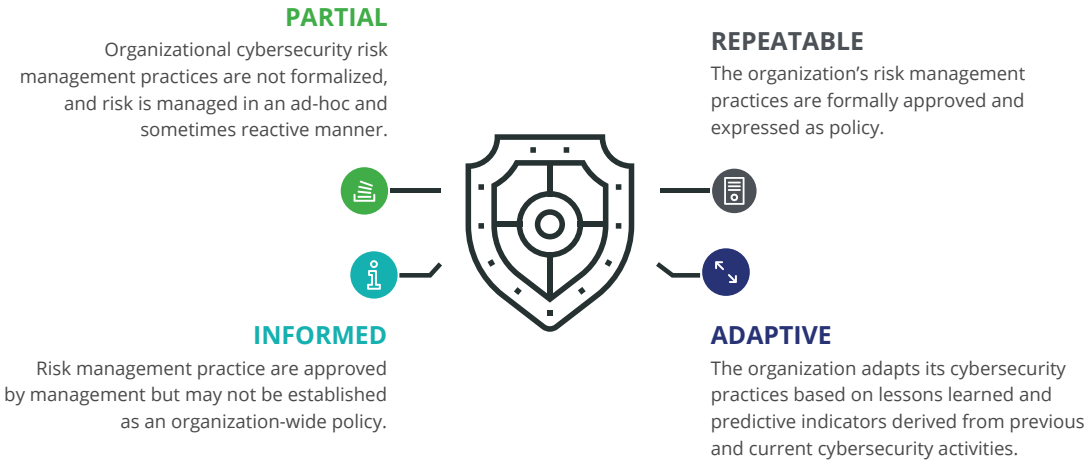
ABOUT THE SURVEY

The survey upon which this article is based was fielded by the Financial Services Information Sharing and Analysis Center (FS-ISAC), in conjunction with Deloitte's Cyber Risk Services practice. Fifty-one companies participated in the pilot launch of the survey, with representation from entities both large (over $2 billion in annual revenue) and small (less than $500 million in revenue), as well as those in between. Respondents came from all financial sectors, albeit skewed more heavily toward the US banking community.

This exploratory study looked at a number of elements in each surveyed financial institution's cybersecurity operation, including how it is organized and governed, who the CISO reports to, the level of board interest in the CISO's work, how much and where it externally sources risk management functions, as well as investment priorities to improve cybersecurity capabilities.

The survey also asked respondents to report on their cybersecurity maturity level, under the four-level National Institute of Standards and Technology (NIST) framework[1] (see figure 1). About half of respondents had their maturity level assessed by a third party, while the remainder were self-assessed. Note that the results presented in this article may not represent the full diversity of practices in the industry due to the small sample size.

Figure 1. Cybersecurity maturity levels



Source: NIST framework[2] as described in the FS-ISAC/Deloitte Cyber Risk Services CISO survey.

Cybersecurity characteristics often differ by maturity level

WHILE it's important to have an adequate budget for cybersecurity, *how a program is organized and governed* may be equally if not more impactful than *how much is spent* relative to a company's overall IT budget or revenue. Indeed, many companies with below average cybersecurity budget allocations managed to achieve a high program maturity level, while some that had higher than average spending were actually less advanced. This dynamic could, in part, reflect the challenges larger, more complex global organizations often face in advancing capabilities versus their smaller counterparts.

If money is not the sole criterion of cybersecurity effectiveness, what factors differentiated the risk management approaches and practices of *adaptive* respondents—those that have reached the highest implementation tier in the NIST framework (see figure 1)—from their lower maturity level counterparts? Here are a few observations:

Accountability starts at the top. Almost all board and management committee members at responding companies were keenly interested in their company's overall cybersecurity strategy. However, those from adaptive companies suggest their boards are more likely to delve into the details of the cybersecurity budget, specific operational roles and responsibilities, as well as the program's general progress than are boards of less advanced peer companies. Respondents from *informed* companies (see figure 1), which fall two tiers below adaptive on the maturity scale, reported their boards were typically significantly less interested in reviewing current threats, program progress, and security testing results.

Shared responsibilities make a difference. More than one-half to three-quarters of respondents, depending on the sector, had a fully centralized cybersecurity function. Among the respondents from the largest participating companies, two-thirds reported a centralized approach. However, respondents from adaptive companies were more likely to favor a hybrid approach—featuring centralized functions, but with each business unit and/or region given strategy and execution capabilities and coordinating with one another.

Multiple lines of defense are maintained. Most respondents from adaptive firms said their organizations tended to have two separate, independent lines of cyber defense—the first involving security at front line units, and the second being organization-wide cyber risk management operations.

Cyber risk exposure is distributed. Nearly one-half of respondents at the informed maturity level said their organizations did not buy any insurance to specifically cover cyber risks. In contrast, two-thirds of those from adaptive companies said their organizations had purchased adequate cyber insurance to cover almost all expected loss scenarios, while one-quarter had insurance to cover at least one-half of their anticipated exposure.

Outside support is sought. Respondents from companies with less mature security programs were more likely to externally source their cybersecurity functions or personnel than were adaptive companies. However, across the board, the most prevalent outside source of help was with "red team" operations, in which a company tests its preparedness to be secure, vigilant, and resilient given the threat of a cyberattack.

Size tends to matter when it comes to cybersecurity programs

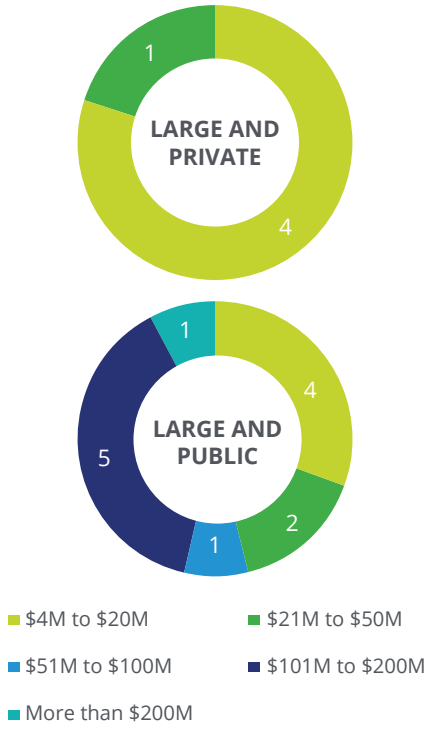
THE study raised a number of other points of distinction when it comes to how larger financial institutions responding to the survey handle their cybersecurity operations. Among the more noteworthy observations:

FSIs may not be allocating enough resources. For the largest FSI companies, analysis of available survey data seems to suggest that their cyber risk management budgets can range anywhere from 5 percent to 20 percent of the total IT budget, with a mean of about 12 percent. In Deloitte's experience working with clients, 20 percent of IT budget is higher than what is designated at most organizations, but this could be attributable either to the method respondents used to account for total spending (capital outlay vs. annual expense) or where they are in their cybersecurity investment program (some could be in a "build" phase, where initial investments are higher but level out over time).

One-half of the large FSI companies reported that cyber risk management spending was $20 million or less. Even if one were to assume these companies invested the most and earned the least revenue within the respective ranges for those categories, this means that one-half are spending one percent or less of revenue on this area. Given the potential operational disruption, reputational damage, investigation and customer costs, and remediation expenses that could emerge from a single successful breach, this may not be enough.[3]

Type of ownership makes a difference. Publicly held FSI companies responding were likely to spend more than their privately owned counterparts for cybersecurity. Among large public FSI companies, about one-third had a budget in the $4 million to $20 million range, while a slightly higher percentage budgeted more than $100 million (see figure 2). This contrasts with respondents from large private FSIs, nearly all of whom indicated that their cybersecurity budgets were in the $4 million

Figure 2. Cyber risk management budgets by FSI company size/type (Private vs. public, with number of respondents cited in each category)



Source: FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

Deloitte Insights | deloitte.com/insights

to $20 million category. This dynamic likely reflects concerns at public financial institutions over a potential multiplier effect from a high-profile breach, which could roil shareholders and analysts as well as undermine market capitalization.

Meat and potatoes over dessert. Survey respondents spent more than two-thirds of their cybersecurity budgets on operational activities, vs. less than one-third on transformational initiatives, with *cyber monitoring and operations* taking up the biggest share of budget and staff allocations (see figure 3). By size, respondents from large companies indicated that less than one-third of their cyber risk management budgets was allocated to transformational initiatives, while those from midsize and smaller companies reported allocating only around one-quarter of budgets to transformation.

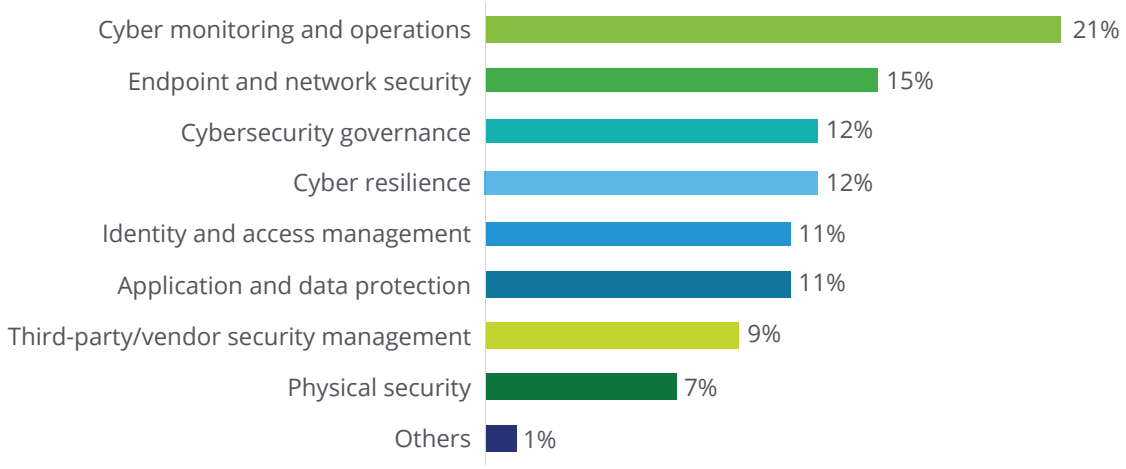
Comparisons to similar measures for IT spending overall vary, but recent research from Ovum suggests that financial services firms spend about 56 percent of total IT budgets on running the business and 44 percent on projects to change the business.[4] Although the way respondents defined "operational" vs. "transformational" may be partly responsible here, our survey sample seems to suggest that spending on cyber risk management may need to pivot to keep up with the level of spending on innovation by the business overall.

CISO reporting relationships vary. According to our survey, company size is likely to be a factor in an FSI's cybersecurity reporting structure. More than one-half of CISOs responding from smaller companies reported directly to the chief executive officer, which likely reflects a flatter organizational structure. At the largest responding companies, the CISO was more likely to report to the chief information officer (CIO), chief operating officer, or chief risk officer (CRO). Half of the midsize respondents said their CISO reports to the CRO.

Innovation is a top priority. Respondents indicated there are clear priorities surrounding which cybersecurity capabilities are most important for investment. Respondents rated mobile, cloud, and data/analytics as the top-three priorities for adoption at their companies in the next two years, while embedding cyber defenses into these new digital initiatives took top rank as the most important business issue with security implications.

When it comes to new investments, survey respondents indicated that innovation and emerging technology are top-of-mind for CISOs, with *cloud, data and analytics*, and *social media* topping the list of technology items that warrant attention at the large firms.

Figure 3. Budget/staff allocations for cyber risk management domains



Source: FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

Where might FSIs go from here?

Lessons learned from the survey and hands-on interaction with companies

WHILE this survey represents a small sample of the financial services community, the results nevertheless indicate steps companies can consider as they continue to upgrade their cybersecurity capabilities and maturity level. In many cases, these observations seem to reinforce the fact that there is a wide spectrum in the maturity of cyber risk management throughout the industry. As a whole, companies should keep raising their game to stay on top of evolving cyber exposures while enabling secure innovation.

To help improve the balance between risk and innovation, financial institutions should consider the following actions:

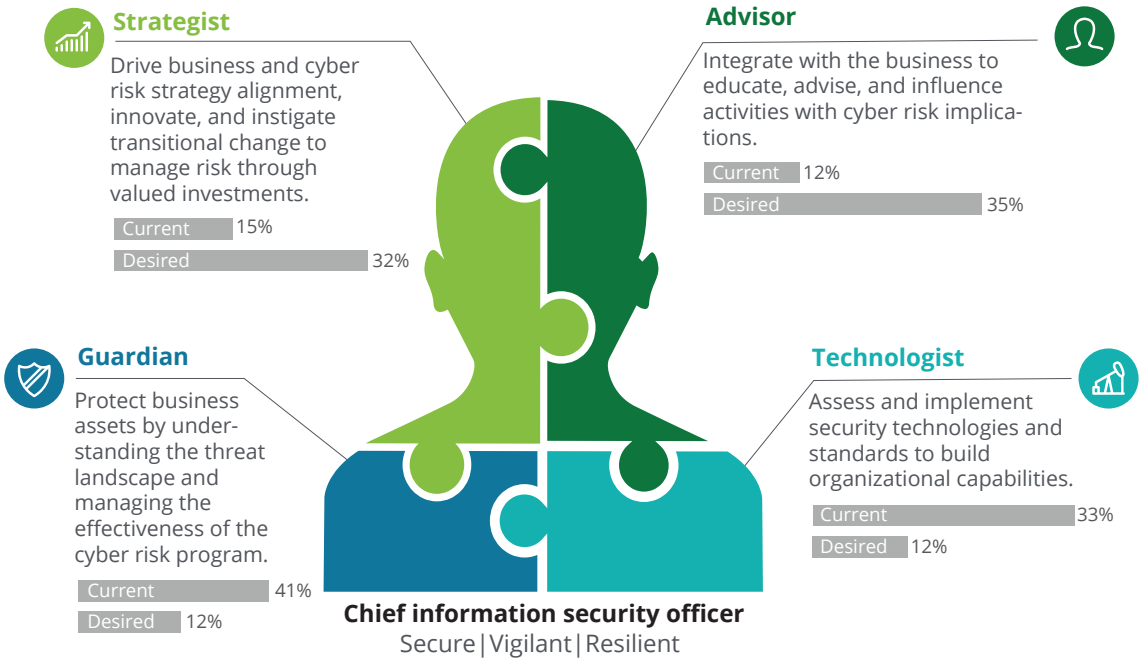
Proactively engage the board. Provide board members with the details of how management is addressing this critical exposure. Their heightened attention will likely not only keep top management more focused on perfecting their approach and improving metrics, but such high-level scrutiny should also resonate throughout the organization.

Engage the entire organization in cybersecurity. With so few full-time employees devoted to cybersecurity, everyone in the organization should understand and embrace their vital role and responsibilities in detecting intrusions, reporting red flags, and maintaining good security hygiene to help prevent events from happening in the first place and limit the damage if they do occur.

Provide multiple lines of defense. Companies should aim to embed cybersecurity practices and personnel within business units and regional offices to support the central cyber risk management team. As it should be everyone's job to manage cyber risk, make sure awareness and duties permeate the organization, and share accountability.

Alter the mix of a CISO's responsibilities. Last but not least, to do their jobs effectively, CISOs should be reporting beyond the CIO and regularly interact outside the IT department. Most CISOs already wear a number of hats, but unfortunately many are often focused on their traditional roles as *technologists* and *guardians* (see figure 4 for a breakdown of responsibilities and definitions). Deloitte's work with CISOs suggests that they spend almost 74 percent of their time in these more tactical roles.[5] As the job has become more complex, however, they should strive to spend two-thirds of their time as *strategists* and *advisors* to better support their management teams and boards.[6]

Figure 4. The four faces of the CISO



Note: Through research conducted at Deloitte's CISO Lab sessions, a divergence was discovered in the time spent in each of the four roles CISOs are performing vs. what is likely to be a more desirable allocation of responsibilities in a world of evolving cyber risks. As indicated above, CISOs should be moving more into strategic and advisory roles, rather than spend the bulk of their time, as they are likely to do currently, as guardians and technologists.[7]

Source: Khalid Kark, Monique Francois, and Taryn Aguas, "The new CISO: Leading the strategic security organization," *Deloitte Review* 19, July 25, 2016.

Deloitte Insights | deloitte.com/insights

Getting to the next level on cybersecurity

AS cybersecurity is expected to continue to be an integral function for financial institutions, improving capabilities will likely be an ongoing challenge as threats keep evolving in scope, technique, and sophistication. FSIs should keep adapting to stay one step ahead of threat actors that intend to do them harm.

At present, we have just scratched the surface when it comes to cybersecurity benchmarking. Future surveys are likely to seek more information on cybersecurity budgets and headcounts by maturity level and company size to create benchmarks such as:

- Maturity score by NIST domain
- Cybersecurity spending as a percentage of IT spending, as well as per FTE
- Number of cyber risk FTEs as a percentage of information security and total IT personnel

However, while benchmarks could help financial institutions assess their readiness to handle cyber risk, remaining secure, vigilant, and resilient also likely requires the industry to look beyond their own experiences and continue working together with broader communities facing the same threats.

As efforts by FS-ISAC demonstrate, collaboration on cybersecurity is important across the financial services industry and within individual industry sectors. At a minimum, financial institutions should closely follow cyber war stories to learn from the experience of peers. This could help FSIs avoid having to reinvent the wheel in efforts to protect their people and systems against the latest cyber threats.

ENDNOTES

1. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 16, 2018.
2. Ibid.
3. Emily Mossburg, J. Donald Fancher, and John Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," *Deloitte Review* 19, July 25, 2016.
4. Informa, *Ovum 2016 ICT enterprise insights survey* (Financial services and payments), accessed May 1, 2018.
5. Khalid Kark, Monique Francois, and Taryn Aguas, "The new CISO: Leading the strategic security organization," *Deloitte Review* 19, July 25, 2016.
6. Deloitte Cyber Risk Services CISO Transition Lab analysis, Deloitte Financial Advisory Services LLP.
7. Ibid.

ABOUT THE AUTHORS

SAM FRIEDMAN

Sam Friedman is the insurance research leader at the Deloitte Center for Financial Services, putting his four decades of industry experience to good use analyzing the latest trends and identifying the major challenges confronting the property-casualty, life insurance, and annuity industries. Friedman joined Deloitte in October 2010 after 29 years at National Underwriter P&C, where he served as editor-in-chief. He has written several articles for Deloitte Insights, and most recently coauthored *Building new ecosystems in middle-market insurance*.

https://www.linkedin.com/in/samoninsurance/

JIM ECKENRODE

Jim Eckenrode is the managing director of the Deloitte Center for Financial Services, where he is responsible for defining the marketplace positioning and development of the Center's eminence and key activities. Eckenrode is frequently a keynote speaker at major industry and client conferences. His most recent publication is *Fintech by the numbers: Incumbents, startups, and investors adapt to fintech evolution*.

https://www.linkedin.com/in/jimeckenrode/

ABOUT DELOITTE CENTER FOR FINANCIAL SERVICES

The Deloitte Center for Financial Services, which supports the organization's US Financial Services practice, provides insight and research to assist senior-level decision-makers within banks, capital markets firms, investment managers, insurance carriers, and real estate organizations.

The Center is staffed by a group of professionals with a wide array of in-depth industry experience as well as cutting-edge research and analytical skills. Through our research, roundtables, and other forms of engagement, we seek to be a trusted source for relevant, timely, and reliable insights. Read recent publications and learn more about the Center on Deloitte.com.

ACKNOWLEDGMENTS

The Center wishes to thank the **Financial Services Information Sharing and Analysis Center (FS-ISAC)** for their help in fielding and analyzing this survey.

The Center wishes to thank the following Deloitte client service professionals for their insights and contributions to this report:

Mark Nicholson, advisory principal, Cyber Risk Services, Deloitte & Touche LLP

The authors also extend special thanks to **Satish Nelanuthula** and **Srinivasarao Oguri** of Deloitte Services India Pvt. Ltd. for their contributions toward the advanced survey analysis in this research project.

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

Prachi Ashani, insurance research analyst, Deloitte Center for Financial Services, Deloitte Support Services India Pvt. Ltd.

Sriram Balakrishnan, advisory manager, Deloitte & Touche LLP

Michelle Canaan, insurance research manager, Deloitte Center for Financial Services, Deloitte Services LP

Michelle Chodosh, senior manager, Deloitte Center for Financial Services, Deloitte Services LP

Patricia Danielecki, senior manager, chief of staff, Deloitte Center for Financial Services, Deloitte Services LP

Nikhil Gokhale, insurance research manager, Deloitte Center for Financial Services, Deloitte Support Services India Pvt. Ltd.

Meghana Rajiv Kanitkar, advisory senior manager, Deloitte & Touche LLP

Erin Loucks, manager, campaign management, Deloitte Services LP

Val Srinivas, research team leader, Deloitte Center for Financial Services, Deloitte Services LP

Katherine Smith, marketing manager, Risk and Financial Advisory, Deloitte Services LP

Carolyn Werner, Deloitte Center for Financial Services Marketing, Deloitte Services LP

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

Executive sponsors
Vikram Bhat
Financial Services Cyber Risk Services leader
Advisory principal
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

Julie Bernard
Advisory principal
Cyber Risk Services
Deloitte & Touche LLP
+1 714 436 7350
juliebernard@deloitte.com

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Karen Edelman, Abrar Khan
Creative: Mahima Dinesh
Promotion: Alexandra Kawecki
Artwork: Neil Webb

About Deloitte Insights
Deloitte Insights 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 Insights is an imprint of Deloitte Development LLC.