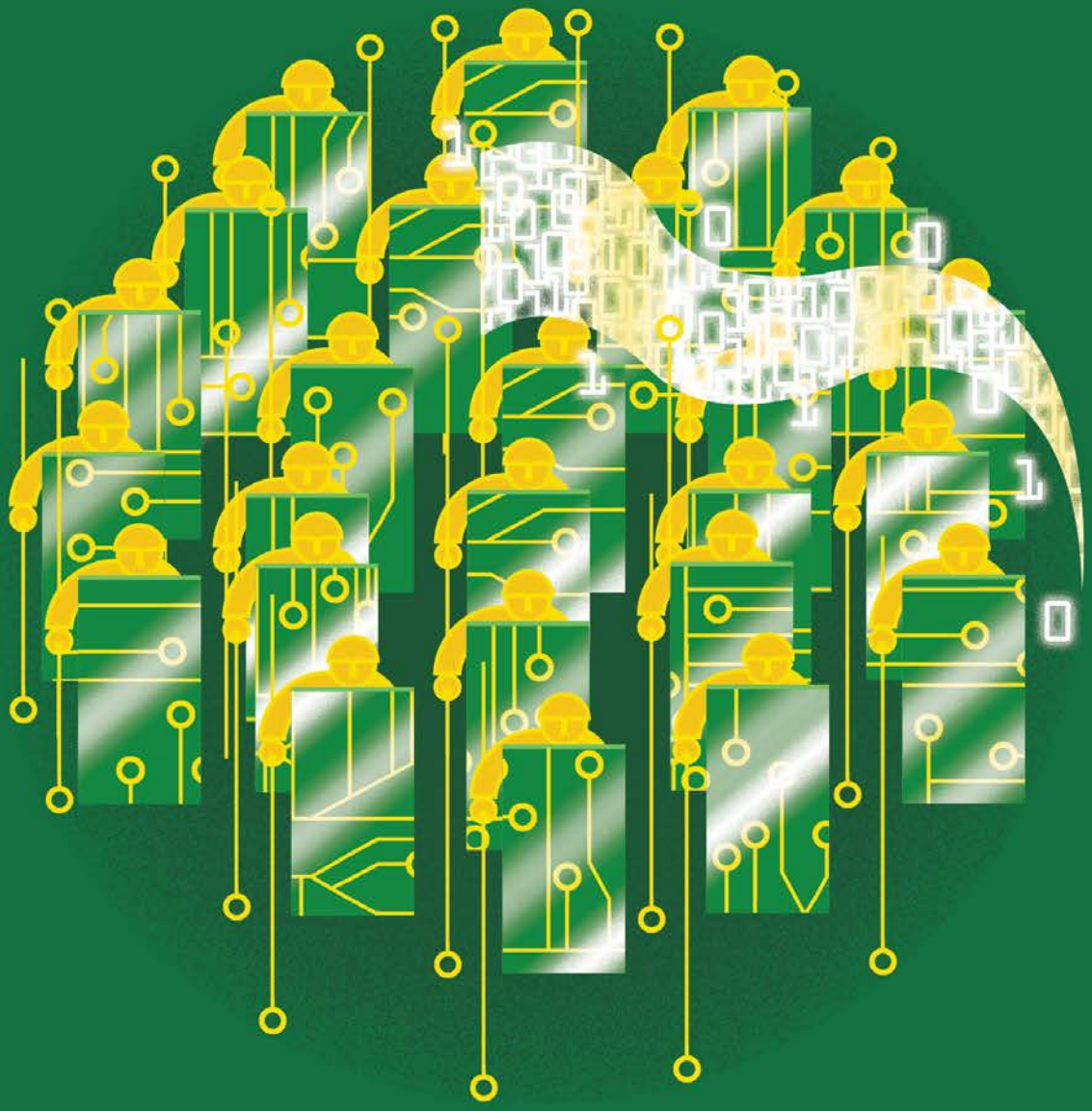
Deloitte. Insights

FINANCIAL SERVICES | Information Sharing and Analysis Center



Pursuing cybersecurity maturity at financial institutions

Survey spotlights key traits among more advanced risk managers

RESULTS AND ANALYSIS FROM THE SECOND ANNUAL FS-ISAC/DELOITTE CYBER RISK SERVICES CISO SURVEY

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

Deloitte Cyber helps organizations create a cyber-minded culture and become stronger, faster, more innovative, and more resilient in the face of persistent and ever-changing cyber threats.

Contents

Top cyber programs exhibit distinct traits

WE ARE ENTERING an era in which digital and physical technologies are more combined and connected than ever. For financial institutions, developing an innate understanding of where and how they could encounter cyber risk in this environment is now of primary importance. At the same time, security teams must continuously strive to fulfill their fiduciary and regulatory responsibilities, while meeting rising expectations for consumer privacy and innovative business solutions.

Over the past two years, Deloitte has worked with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to survey members on how they are confronting these cyber challenges. The objective is to measure good stewardship of both the cybersecurity budget and overall cyber risk management program.

Our 2018 pilot provided a snapshot of how the chief information security officers (CISOs) who responded to our survey were discharging their responsibilities, while offering preliminary insights into the industry's broad spectrum of cybersecurity strategies, structures, and budget priorities.[1] This year—in addition to identifying spending patterns across the industry by sector, size of company, and cyber risk management maturity level—we identified several core traits of those that have already reached the highest maturity level as defined by the National Institute of Standards and Technology (NIST). (See figure 1.)

These defining characteristics of "adaptive" companies, which are alluded to in the NIST cybersecurity maturity framework,[2] include:

- Securing the involvement of senior leadership, both top executives and the board;
- Raising cybersecurity's profile within the organization beyond the information technology (IT) department to give the security function higher-level attention and greater clout; and
- Aligning cybersecurity efforts more closely with the company's business strategy.

FIGURE 1

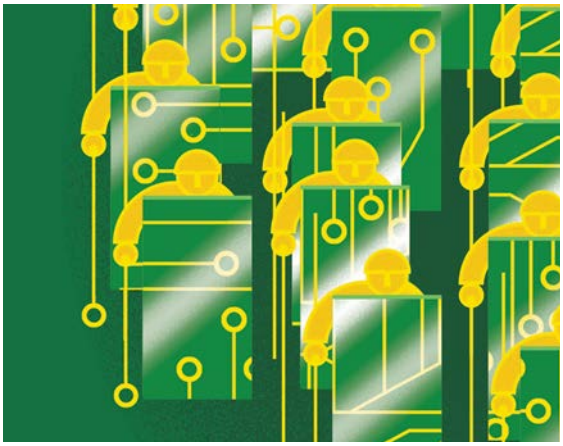
Cybersecurity maturity levels

Partial	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.
Informed	Risk management practices are approved by management but may not be established as policy across the organization.
Repetitive	The organization's risk management practices are formally approved and expressed as policy.
Adaptive	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.

Source: National Institute of Standards and Technology (NIST), "Framework for improving critical infrastructure cybersecurity," April 16, 2018.

Organizations that can integrate these fundamental elements and follow the example set by leading cybersecurity programs will more likely become and remain adaptive in the face of an ever-evolving business and threat landscape.

The survey indicated that money alone is probably not the answer, as higher cybersecurity spending did not necessarily translate into a higher maturity level. That likely means exactly how—and how well—financial institutions go about securing their digital fortress is at least as important as the amount of money devoted to cybersecurity.



Spotlight on spending

UNDERSTANDING THE RESOURCES that firms devote to cyber risk was one of the more important data points we wanted to gather from this effort (figure 2). Those responding to the survey spent anywhere from 6 percent to 14 percent of their IT budget on cybersecurity, with an average of 10 percent. This amount translated to a range of around 0.2 percent to 0.9 percent of company revenue, with an average of about 0.3 percent. In terms of spending per employee, respondents spent between US$1,300 to US$3,000 per full-time or equivalent employee (FTE) on cybersecurity, with an average of around US$2,300.

The ranges represent the diversity we saw in the sample—varying, for example, by the size of the responding company (figure 3).

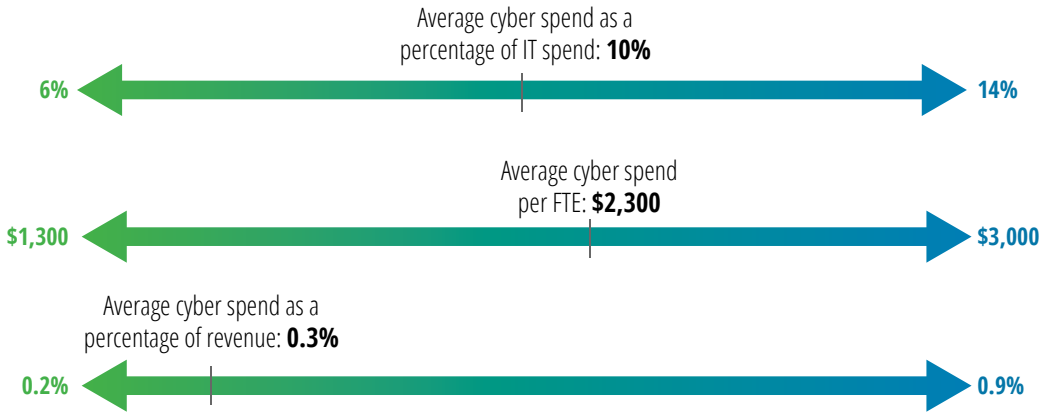
At first glance, it appears smaller companies have some catching up to do to match the financial commitment of larger respondents. Small institutions surveyed spent a lower percentage of their revenue (0.2 percent) on cyber than did midsize (0.5 percent) or large companies (0.4 percent), and while their average spending of US$2,100 per FTE matched that of midsize firms, it is far lower than the US$2,700 cited by their large counterparts. That could be explained by the greater complexity of larger institutions, which often offer more products and services and have multiple business units and delivery channels to account for.

Smaller companies surveyed did commit a higher percentage of their IT budget (12 percent) to cybersecurity than did large and midsize firms (9 percent). This may indicate that smaller firms realize they need to commit a larger piece of the IT pie to meeting new regulatory requirements and operational needs on cyber.

Digging deeper into spending decisions, larger firms allocated nearly one-fifth of their cybersecurity budget to identity and access management—nearly twice the percentage of midsize and smaller

FIGURE 2

Average cybersecurity spending range at financial institutions (overall sample)



Note: All dollar amounts are given in US dollars.

Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

FIGURE 3

Financial institutions' average cybersecurity spending, by company size

	Small	Midsize	Large
Cyber spend as a percentage of IT spend	12%	9%	9%
Cyber spend per FTE	$2,100	$2,100	$2,700
Cyber spend as a percentage of revenue	0.2%	0.5%	0.4%

Note: All dollar amounts are given in US dollars.
Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

companies, which tended to spend more heavily on endpoint and network security. (For more about how respondents compared based on their revenue segment, see the sidebar, "Size drives divergent strategies" on pages 13–14.)

There were also differences by industry segment. For example, bank respondents reported that they allocated a slightly higher than average percentage (close to 11 percent) of their IT budget to cybersecurity, while insurance and nonbanking financial services companies were slightly below the overall respondent average of 10 percent—although at around 0.33 percent, all three were nearly even as a percentage of company revenue. Yet in terms of dollars spent per FTE, nonbanking financial services companies allocated considerably more—about US$2,800—than did banks (about US$2,000) or insurers (nearly US$2,200).

The highest spending group among this survey sample were the financial utilities, such as clearinghouses, exchanges, and payment processors, which averaged around 15 percent of their IT budget on cybersecurity, 0.75 percent of revenue, and about US$3,600 per FTE. Service providers (financial products/services/applications) also reported spending slightly more, at nearly 11 percent of the IT budget and about 0.60 percent of revenue, yet only averaged US$2,000 or so per FTE—about the same as bank respondents.

Most interestingly, while there were slight differences in spending by maturity level, adaptive companies did not necessarily spend more than the sample's overall average on their cybersecurity programs. This is in line with our central theme: *How* a security program is planned, executed, and governed is likely as important as *how much money* is devoted to cybersecurity. So, what differentiates adaptive companies in their cybersecurity approaches?

Defining characteristics of advanced cybersecurity programs

CISOS WORK THROUGH a multitude of systems and processes in their ongoing efforts to secure their organizations against cyber intrusions, establish heightened vigilance to spot attacks before they can do serious harm, and be resilient when recovering from a significant event. With so many varied risk management activities going on simultaneously, CISOs at times may find it difficult to prioritize their efforts. What fundamental elements should be in place to accelerate a financial institution's cybersecurity maturity and maintain a high level once it is attained?

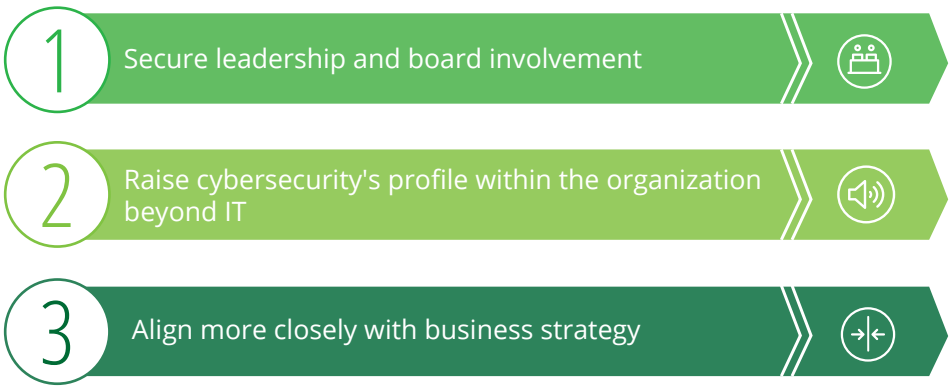
While there are many factors that go into making a cybersecurity program successful, we found three common denominators that typically separate adaptive companies from the rest. Adaptive companies were generally best able to: 1) secure executive leadership and board involvement; 2) raise cybersecurity's profile beyond the IT department; and 3) align cyber risk management more closely with business strategy (figure 4).

These findings conform to the NIST description of what an adaptive organization looks like. That is encouraging, because almost all the respondents who classified their organizations as "adaptive" did so with a self-assessment, meaning they fully appreciate what they needed to do to indeed reach the highest maturity level.

These adaptive companies can serve as a role model for less mature organizations aiming to reach the next level. Financial institutions that can successfully emulate these defining characteristics are likely to improve their cybersecurity maturity in the short term as well as continue to bolster their defenses over the long haul.

FIGURE 4

The three characteristics that set adaptive companies apart



Source: Deloitte Center for Financial Services analysis of survey responses.

By emulating adaptive companies, CISOs can also expand beyond their traditional roles as technologists and guardians. This can enable them to devote more time as strategists and advisors to better support the broader operations and goals of their business units, management teams, and boards.[3]

Characteristic No. 1: Secure leadership and board involvement

Adaptive companies, as defined by NIST, call for senior executives to monitor cybersecurity risk in the same context as financial risk and other organizational risks.[4] That certainly tracks with our survey's finding that *lack of management support/ inadequate funding* was cited as a CISO's top challenge in managing cybersecurity by companies with a lower (*informed*) level of maturity.

Our analysis went beyond senior executives, finding that the boards and management committees of those survey respondents who classified themselves as adaptive were more interested in nearly all areas of cybersecurity than were those at the informed level (figure 5). Indeed, boards and management committees at the lowest maturity companies appear to be interested in fewer areas of cybersecurity activities.

FIGURE 5

Adaptive companies typically have a more engaged board

	Adaptive	Repetitive	Informed
Overall security strategy	14	33	7
Security budget	6	19	6
Security policies	5	11	3
Review of current threats and security risks	13	31	7
Review roles and responsibilities of security organization	3	6	0
Review of security testing results	11	24	6
Security technologies	3	5	1
Program progress	12	29	4
Review of whether the organization is vulnerable to another organization's public breach	11	27	5
Others	0	3	1
Total responses	17	42	14

Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

By comparison, interest rises dramatically among the next level up on the maturity curve ("repetitive"), from *overall security strategy* to *reviews of threats and security risks*, *cybersecurity program progress*, *vulnerability to a third-party breach*, as well as *review of security testing results*. In most areas, board and management committee interest peaks among adaptive companies.

Adaptive respondents were more likely to elevate the cybersecurity function by completely segregating cybersecurity from IT.

Better education of the board and the management committee by CISOs and other C-suite executives around current threats and security risks and their implications for the business could galvanize increased engagement. Having an engaged board that works closely with senior management on cybersecurity issues can help focus the entire organization on the challenge while assuring that adequate resources are allocated to the task.

For example, the survey found that five out of 14 adaptive companies compared to only one in 12 informed ones assigned a high priority to *investing in organizationwide awareness and training*, something that requires resources and support from multiple functions. More adaptive companies tend to be better able to engage and enlist the whole organization across all functions and embed security-minded practices into day-to-day work routines, from new product development to customer service to core processes.

Characteristic No. 2: Raising cybersecurity's profile within the organization beyond IT

Cybersecurity as a discipline originated within the IT function. Therefore, it is not surprising that one-half of all respondents—including those from adaptive companies—reported that the security team was part of the IT function at their organization. After all, a company's technology systems are not only the target of cyberattacks, but a large part of the solution in preventing intrusions from succeeding and limiting the damage if they do.

That said, cyber threats are increasingly being acknowledged as one of the most critical risk exposures facing an organization, and cybersecurity today is not merely a technology challenge. More mature companies have therefore recognized the need to raise the profile of the security function, enabling decisions that are above and independent of other IT considerations or constraints.

The survey findings (figure 6) showed that adaptive respondents were more likely to elevate the cybersecurity function by completely segregating cybersecurity from IT. Repetitive respondents appear to be moving in this direction; their organizations were more likely to segregate the two functions but still maintain common lines of reporting. Informed respondents were by far the most likely to keep cybersecurity as part of IT, and least likely to split the functions and give cyber a separate identity.

In addition, about one-half of adaptive companies (nine out of 17) operated a first line and second line of defense with complete independence, versus only two out of 14 of informed respondents.

The theme of raising cybersecurity's profile and segregating it from IT was also reflected in the reporting structure at adaptive companies surveyed (figure 7), where more CISOs reported to chief operating officers (COOs) and chief risk officers (CROs) than to chief information officers (CIOs) and chief technology officers (CTOs).

The survey also found that nearly all the CISOs at adaptive companies reported no lower than two levels down from the chief executive officer (CEO), compared with three of four at repetitive organizations, and two of three among informed respondents.

That said, across the complete sample surveyed, very few CISOs reported to a general counsel or a chief compliance officer (CCO). This indicates that

FIGURE 6

More mature programs moving toward segregation of IT and cybersecurity

	Adaptive	Repetitive	Informed
IT and cybersecurity functions are completely segregated	4	5	1
IT and cybersecurity functions are segregated but have common lines of reporting	1	10	2
IT and cybersecurity personnel have shared security responsibilities	3	11	1
Cybersecurity function is part of the IT organization	9	17	10
Total responses	17	43	14

Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

FIGURE 7

To whom does the chief information security officer (CISO) or equivalent report?

	Adaptive	Repetitive	Informed
Chief executive officer (CEO)	2	5	2
Chief financial officer (CFO)*	1	1	1
Chief information officer (CIO)*	2	10	7
Chief technology officer (CTO)*	1	5	0
Chief risk officer (CRO)*	4	6	0
Chief compliance officer (CCO)*	0	0	1
Chief operating officer (COO)*	5	6	3
Chief privacy officer*	0	1	0
General counsel	1	3	0
Others	1	6	0
Total responses	17	43	14

*Or equivalent

Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

most cybersecurity programs at financial institutions have moved beyond just compliance; they are becoming a part of the broader security function responsible for combating cyber risk and are touching every part of the organization. For most progressive CISOs, the next step would likely be providing strategic inputs during the business planning and decision-making phases.

Characteristic No. 3: Aligning cybersecurity more closely with business strategy

In today's increasingly digital and data-driven world, business functions across the board rely heavily on technology to carry out day-to-day operations internally and externally. How well companies leverage emerging technology to innovate and change the way they operate is often what differentiates them from competitors.

New technology, however, may also expose companies to additional cyber vulnerabilities. For example, most respondents said the top two emerging technologies their companies plan to adopt over the next two years were cloud and data analytics. Yet as Deloitte's *2019 Insurance Outlook* noted, as insurers increase cloud usage to speed up transformation and free up resources, regulators have been raising concerns about the potential for cybersecurity issues, because core systems and critical data are essentially being moved offsite to a third party.[5] While service providers are accountable for the security of their hardware and software, the ultimate responsibility for ensuring cybersecurity of cloud functions remains with the insurer, and any breach of cloud data could have regulatory and reputational implications for the company.[6]

Bank CISOs often face similar challenges. "As more data is used in AI applications, concerns over data protection and privacy could escalate institutions' risk profile," noted Deloitte's *2019 Banking Outlook*. "Increased connectivity with third-party providers and the potential for increased cyber risk is another growing concern."[7]

Adaptive respondents already seem to recognize that cybersecurity needs to be more closely tied to overall strategy, as *business growth and expansion* was identified as their second biggest challenge when managing cybersecurity (figure 8), trailing only *rapid IT changes and rising complexities*—an issue that faces all CISOs, regardless of company maturity level. As companies grow by adding new platforms, products, geographic regions, apps, and Web capabilities, cybersecurity considerations can multiply along with the introduction of each new element.

In contrast, companies with less mature cybersecurity programs were often still contending with much more basic issues than how to cope with growth challenges. The second largest problem repetitive companies face, for instance, is *prioritizing options for securing the enterprise*, while the biggest challenge facing informed respondents was *lack of management support and inadequate funding*.

Better alignment with business plans will likely help CISOs identify and respond to emerging exposures. Those from adaptive and repetitive

FIGURE 8

Adaptive companies are more aware of the implications of business expansion on cybersecurity

Ranking of cybersecurity challenges

	Overall	Adaptive	Repetitive	Informed
Rapid IT changes and rising complexities	1	1	1	2
Business growth and expansion	2	2	4	5
Excessive focus on compliance with regulations, and lesser on cyber risk management	3	3	5	6
Unavailability of skilled cyber professionals	4	6	3	4
Difficulty to prioritize options for securing the enterprise	5	5	2	6
Inadequate functionality and interoperability of security solutions	6	4	6	10
Lack of management support/inadequate funding	7	7	8	1
Poor understanding of cyber risks and security	8	8	7	9
Inadequate governance	9	9	9	3
Lack of cybersecurity strategy	10	10	10	8

Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

companies recognized third-party/supply chain control deficiencies as one of the top three cybersecurity threats to their organization. Respondents from informed companies, meanwhile, seemed to be grappling with more internal issues, such as unauthorized access to systems, as well as inadequate detection and response capabilities.

Embedding cyber professionals into strategic initiatives and transformational projects right from the onset will likely help the security function better manage cyber risk across the enterprise and foster greater collaboration and innovation.[8]

Cybersecurity maturity should be an ongoing effort

THERE ARE MANY other factors beyond the maturity level to consider when examining a financial institution's cybersecurity program. Size is one such consideration (see sidebar, "Size drives divergent strategies"); another is industry sector.

Yet no matter how an institution stacks up against its competitors or how those comparisons are made, cybersecurity will remain a work in progress for all financial organizations. Indeed, regardless of who is ultimately in charge and how governance is structured, cybersecurity awareness, responsibility, and accountability should be part of every department within every financial services firm.

Even highly mature companies should keep adapting

Respondents from adaptive companies should not rest on their laurels. While the survey indicated that high maturity respondents may have settled on a solid governance system and laid the foundation for an effective cyber risk management program, there's likely still much work to be done to keep fortifying defenses and response capabilities.

As noted, even adaptive companies are racing to keep up with *rapid IT changes and rising complexities in tech systems*, which was cited as a top challenge for CISOs regardless of company size or maturity level. Such efforts have taken on a new sense of urgency in this age of heightened consumer sensitivity about data security and privacy, as well as additional regulatory demands.

Achieving excellence in cybersecurity will therefore likely remain an ongoing journey, with many twists and turns, rather than an ultimate destination. Cyberattacks continue to be bolder and more sophisticated, challenging financial institutions to respond in kind. Companies will need to continuously upgrade their capabilities—both human and technological—to remain secure, vigilant, and resilient.

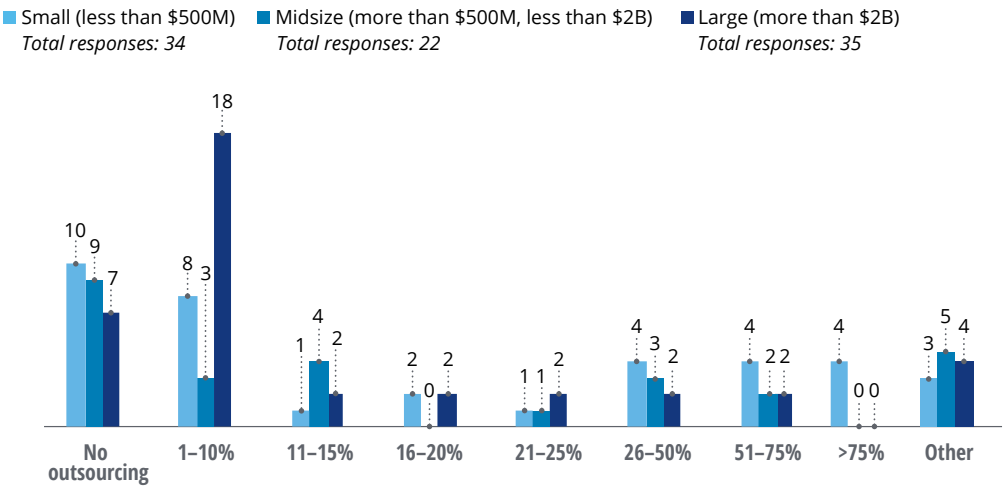
CISOs should also keep getting better at being proactive, anticipating potential exposures and preparing to counter them, rather than reacting to new modes of attack as they arise. Even an adaptive organization could be vulnerable without a sustained effort to stay one step ahead of those seeking to penetrate its digital fortress and compromise its operations.

SIZE DRIVES DIVERGENT STRATEGIES

The size (by annual revenue) of responding companies made a difference when it came to many of the characteristics addressed in our survey. For example, larger respondents were far more likely to keep all their cybersecurity functions in-house, and similarly were least likely to outsource their cybersecurity workforce (figure 9).

FIGURE 9

Percentage of cybersecurity workforce that is outsourced, by company annual revenue



Note: All dollar amounts are given in US dollars.

Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

Larger companies also tended to keep their CISOs within IT: 56 percent of respondents at these companies said their CISO reported to the CIO or CTO rather than to the CRO or COO, compared to about one in four midsize and small companies (figure 10). Perhaps due to their relatively flatter organizations, respondents from smaller companies were most likely to have their CISOs report to the CEO, with one in four respondents doing so. Meanwhile, only a handful of midsize company respondents said their companies had CISOs reporting that high up the corporate ladder, and none of the respondents from larger companies responded this way.

Larger company respondents were more likely to attempt a hybrid operating model—with strategy and execution capabilities in both a centralized function and at each business or region. Here, both functions were integrated and worked in coordination with one another. However, such an approach remained the exception rather than the rule at all revenue levels, with a little more than one in 10 large companies going this route, and far fewer than that among midsize and smaller firms.

Respondents from larger companies were also more likely to have an independent second line of cyber defense, and to have cybersecurity interface with the business via security liaisons or "champions" within each unit.

Risk transfer was another differentiator, as fewer than one in 10 large company respondents are operating without cyber insurance, versus one in four midsize companies. These respondents also had relatively more mature programs overall. Eight out of the 23 large company respondents that

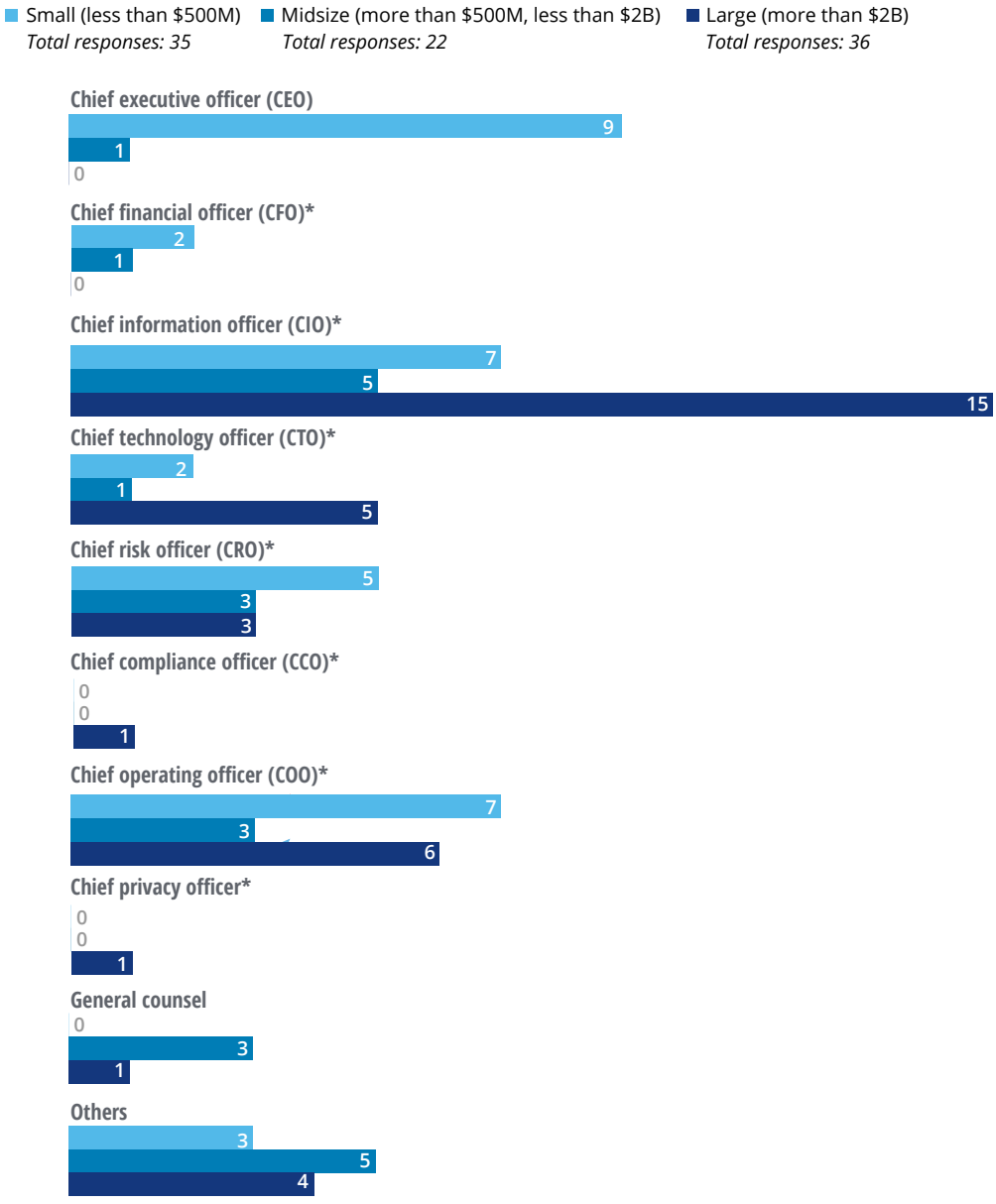
continued >

SIZE DRIVES DIVERGENT STRATEGIES, CONT.

disclosed their program maturity characterized themselves as adaptive, 13 were repetitive, and two were informed. Of the 20 who were from midsize organizations, only two firms were in the adaptive category, versus 14 repetitive and four informed. Of the 31 respondents from small companies, seven said their companies were adaptive, 16 were repetitive, and eight were informed.

FIGURE 10

To whom the CISO reports, by company annual revenue



*Or equivalent

Note: All dollar amounts are given in US dollars.

Source: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

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 in the fall of 2018. Ninety-seven companies participated, with representation spanning multiple revenue levels (figure 11) and all financial sectors (figure 12, adding up to more than 97 because some respondents represented multiple categories).

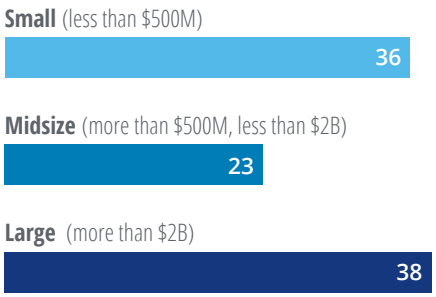
The study looked at various components of a financial institution's cybersecurity operation, including how it is organized and governed, who the CISO reports to, the level of board interest in the CISO's work, as well as which cybersecurity capability areas were prioritized in terms of spending.

The survey also asked respondents to report on their cybersecurity maturity level under the four-level NIST framework[9] (figure 1). Eight out of 10 respondents self-assessed their maturity level, while the remaining were third-party assessments. Out of 97 survey participants, 74 responded with their assessment of maturity levels for each of the 16 NIST parameters.

Based on a calculated combination of maturity ratings for each of the parameters, 17 companies were identified as having reached an adaptive level of maturity, 43 companies were repetitive, 12 were informed, and two were partial. Companies that fell into the partial maturity level were grouped with companies in the informed maturity category to ensure analytical rigor for the purposes of this report.

FIGURE 11

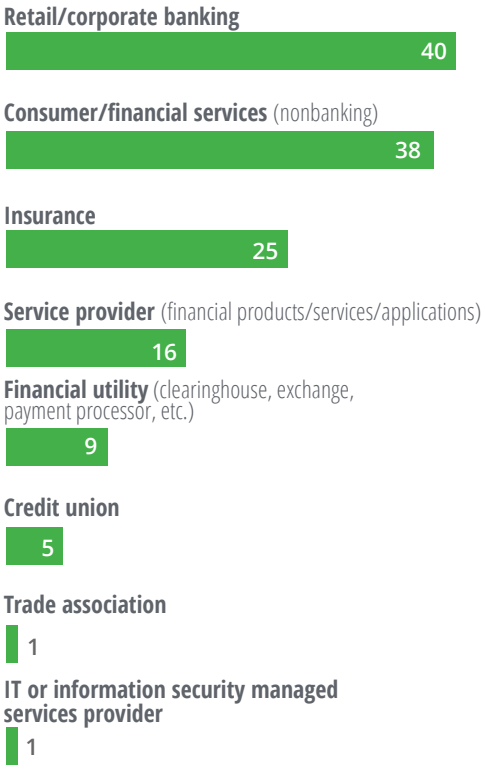
Respondents by revenue



Note: All dollar amounts are given in US dollars.

FIGURE 12

Respondents by industry



Sources: 2019 FS-ISAC/Deloitte Cyber Risk Services CISO survey, Deloitte Center for Financial Services analysis.

Endnotes

1. Jim Eckenrode and Sam Friedman, *The state of cybersecurity at financial institutions: There's no "one size fits all" approach*, Deloitte Insights, May 21, 2018.
2. National Institute of Standards and Technology (NIST), "Framework for improving critical infrastructure cybersecurity," April 16, 2018.
3. Khalid Kark, Monique Francois, and Taryn Aguas, "The new CISO: Leading the strategic security organization," *Deloitte Review* 19, July 25, 2016.
4. NIST, "Framework for improving critical infrastructure cybersecurity."
5. Sam Friedman et al., *2019 insurance outlook*, Deloitte, November 2018.
6. Ibid.
7. Val Srinivas et al., *2019 banking and capital markets outlook*, Deloitte, November 2018.
8. Deloitte, *The future of cyber survey 2019*, March 4, 2019.
9. NIST, "Framework for improving critical infrastructure cybersecurity."

About the authors

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 *Closing the gap in fintech collaboration: Overcoming obstacles to a symbiotic relationship*. Connect with him onLinkedIn at www.linkedin.com/in/samoninsurance/.

NIKHIL GOKHALE, Deloitte Services India Pvt. Ltd., is a research specialist at the Deloitte Center for Financial Services, where he covers the insurance sector. He focuses on providing insights to large financial institutions on strategy, technology, and performance issues. Prior to Deloitte, he worked as a senior research consultant on strategic projects relating to postmerger integration, operational excellence, and market intelligence. Connect with him on LinkedIn at www.linkedin.com/in/nikhil-gokhale-620ab93.

Acknowledgments

The center wishes to thank **Prachi Ashani**, contributing data analyst, for her contributions to this report. The center also wishes to thank the **Financial Services Information Sharing and Analysis Center (FS-ISAC)** for their help in fielding and analyzing this survey.

The authors also extend special thanks to **Satish Nelanuthula**, **Srinvarsarao Oguri**, and **Soumva Mohapatra** 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:

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

Christopher Faile, public relations leader, financial services, Deloitte Services LP

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

Erin Loucks, manager, campaign management, Deloitte Services LP

Swati Nidiganti, advisory manager, Deloitte & Touche LLP

Venkat Chalam Pogaru, advisory assistant manager, Deloitte & Touche LLP

About the 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 experiences 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.

Contacts

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

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

AUTHORS
Sam Friedman
Insurance research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Nikhil Gokhale
Insurance research manager
Deloitte Center for Financial Services
Deloitte Support Services India Private Limited

Deloitte.
Insights

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

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Karen Edelman, Blythe Hurley, and Abrar Khan
Creative: Emily Moreano
Promotion: Hannah Rapp
Cover 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.

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.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2019 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited