Deloitte. Insights

FS-ISAC

Reshaping the cybersecurity landscape

How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions

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. For weekly actionable insights on key issues for the financial services industry, check out the Deloitte Center for Financial Services' QuickLook article series.

Connect

To learn more about the vision of the DCFS, its solutions, thought leadership, and events, please visit **www.deloitte.com/us/cfs.**

Subscribe

To receive email communications, please register at **www.deloitte.com/us/cfs**.

Engage

Follow us on Twitter at: **@DeloitteFinSvcs**.

About FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an industry consortium dedicated to reducing cyber risk in the global financial system. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats. FS-ISAC has nearly 7,000 member firms with users in more than 70 countries. Headquartered in United States, the organization has offices in the United Kingdom and Singapore. To learn more, visit www.fsisac.com. To get clarity and perspective on the future of finance, data, and cybersecurity from top C-level executives around the world, visit FS-ISAC Insights.

Contents

KEY FINDINGS

- Survey respondents reported an increase in cybersecurity spending, with identity and access management, cyber monitoring and operations, and endpoint and network security receiving bigger shares of the pie.
- For the last three years, respondents identified *rapid IT changes and rising complexities* as their No. 1 cybersecurity challenge. To help effectively mitigate emerging cyber risks, companies should consider digitally enabling the cyber function within the broader IT service development process. Adopting "security by design" principles during technology development could also help financial institutions create more secure products.
- Cybersecurity is often included as part of the IT function, and CISOs typically report to the CIO or CTO at their firms, according to most respondents from large financial institutions surveyed. This reflects the need for close integration of cybersecurity and IT.
- At the same time, financial institutions may want to retain a certain level of independence for cybersecurity, which could help ensure risk management decisions are not overshadowed by IT constraints.
- Respondents cited emerging technologies such as cloud, data analytics, and robotic process automation as top cybersecurity investment priorities. Access control, protective technology, and data security were emphasized as rationales.
- As digitization and remote work accelerates, and lines among employees, customers, contractors, and partners/vendors are blurring, many traditional network perimeters and boundaries are obscured. Users, workloads, data, networks, and devices are everywhere. "Zero Trust" has emerged as a concept for enforcing "least privilege" for modern enterprises contending with the ubiquitous nature of these domains.

Time to double down on cybersecurity

MOST FINANCIAL INSTITUTIONS have been moving steadily toward digitization for some time now. Operations across companies large or small in all financial sectors have been going digital, driven by the need for efficiency as well as rising customer expectations. Among financial services firms, the pace of adoption has often varied based upon a company's readiness for change, agility, and size, among other factors.

Over the last few months, the COVID-19 pandemic has forced many companies to accelerate their digitization efforts. As office closures and restricted movement compelled everyone and everything that could go virtual to do so, many institutions had to more fully embrace a digital transformation in operations, distribution, and customer engagement.

This sudden shift, however, has compounded problems for many chief information security officers (CISOs) and cybersecurity teams charged with securing the digital fortress at their firms. Hackers and cyber scammers are trying to take advantage of expanding technology footprints and new attack surfaces, with most employees working remotely. In April, the New York Department of Financial Services highlighted the significant increase in cybercrime related to the COVID-19 outbreak.[1]

The imperative is clear across the board: Organizations should be digitally enabling the cybersecurity function to keep pace with rapid IT transformation and protect critical assets against increasing levels of cyberthreats and attacks. For the third consecutive year, the Cyber & Strategic Risk Services team at Deloitte & Touche LLP and the Financial Services Information Sharing and Analysis Center (FS-ISAC) surveyed FS-ISAC members on how they are confronting cyber challenges. (The most recent survey was fielded from late 2019 through January 2020, and the results will be referred to as the 2020 survey report. Each year, we identify and present the particular survey results according to their year of publication—2020, 2019, and 2018. (See sidebar, "About the survey," for further details.)

Our annual survey explores how cybersecurity programs are structured and managed at financial institutions and the different choices made in terms of organization models, spending patterns, outsourcing, and investment priorities, among other important considerations.

Over the past three years, cybersecurity has continued to grow as a priority. Financial firms keep allocating more resources, increasing board involvement, and making investments that are more aligned to IT and business priorities. The report also identifies several key cyber risk management trends at large financial institutions, as well as future implications that may be relevant to firms of all sizes in the wake of COVID-19.

Spending rises to meet increased demand

ONE OF THE most important components of a financial institution's cyber risk management operation is the level of resources allocated to cybersecurity programs. The average annual cost of cyberattacks has been ballooning for many organizations.[2] So, it was not surprising to find that cybersecurity spending rose among the financial institutions surveyed compared to those responding in the prior year (figure 1).

Respondents to our most recent survey spent about 10.9% of their IT budget on cybersecurity on average, up from 10.1% a year earlier. This equaled about 0.48% of company revenue on average, again up from 0.34%. In terms of spending per employee, respondents spent about US$2,700 on average per full-time employee (FTE) on cybersecurity, increasing from about US$2,300 last year.

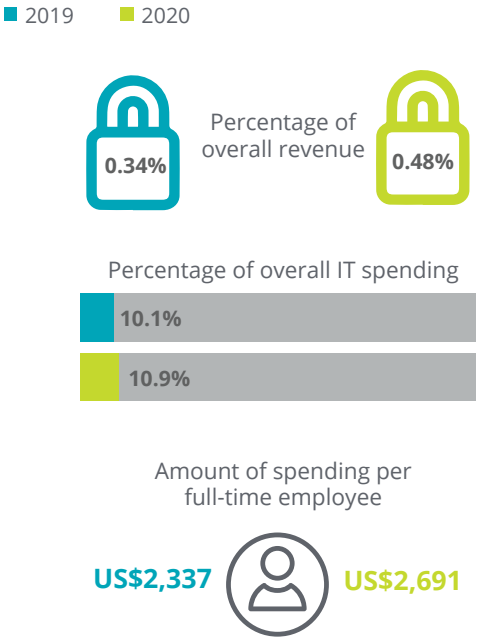
At the same time, cybersecurity spending by sector has changed significantly across different benchmarks (figure 2).

Despite increased spending, budget allocations have remained largely consistent over the three years of the survey. Cyber monitoring and operations, endpoint and network security, and identity and access management collectively received more than 50% of the spending pie in our latest survey (figure 3).

FIGURE 1

Companies continue to spend more on cybersecurity

Overall cybersecurity spending benchmarks



Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

FIGURE 2

Cybersecurity spending across sectors

Percentage of revenue | Percentage of IT spending | Per FTE

	2019	2020
Retail/corporate banking	0.3% 10.1% US$2,074	0.6% 9.4% US$2,688
Consumer/financial services (nonbanking)	0.3% 9.7% US$2,817	0.4% 10.5% US$2,348
Insurance	0.3% 9.3% US$2,245	0.4% 11.9% US$1,984
Service provider	0.6% 8.9% US$1,956	0.6% 7.2% US$3,226
Financial utility	0.8% 15.2% US$3,630	0.8% 8.2% US$4,375
Aggregated total	0.3% 10.1% US$2,337	0.5% 10.9% US$2,691

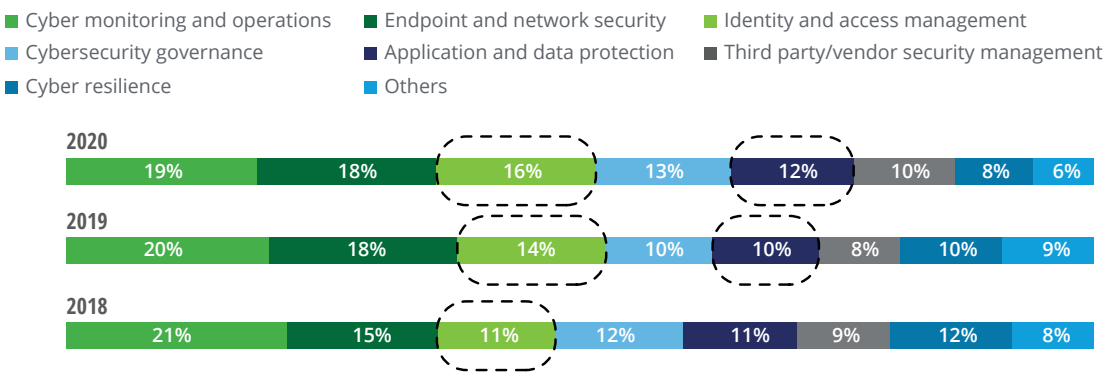
Note: FTE=Full-time employee or equivalent.

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

FIGURE 3

Budget allocations have remained largely consistent across different cybersecurity domains, with a couple of notable exceptions

Budget allocation across cybersecurity domains by survey respondents



Note: Percentage totals may not equal 100% due to rounding.

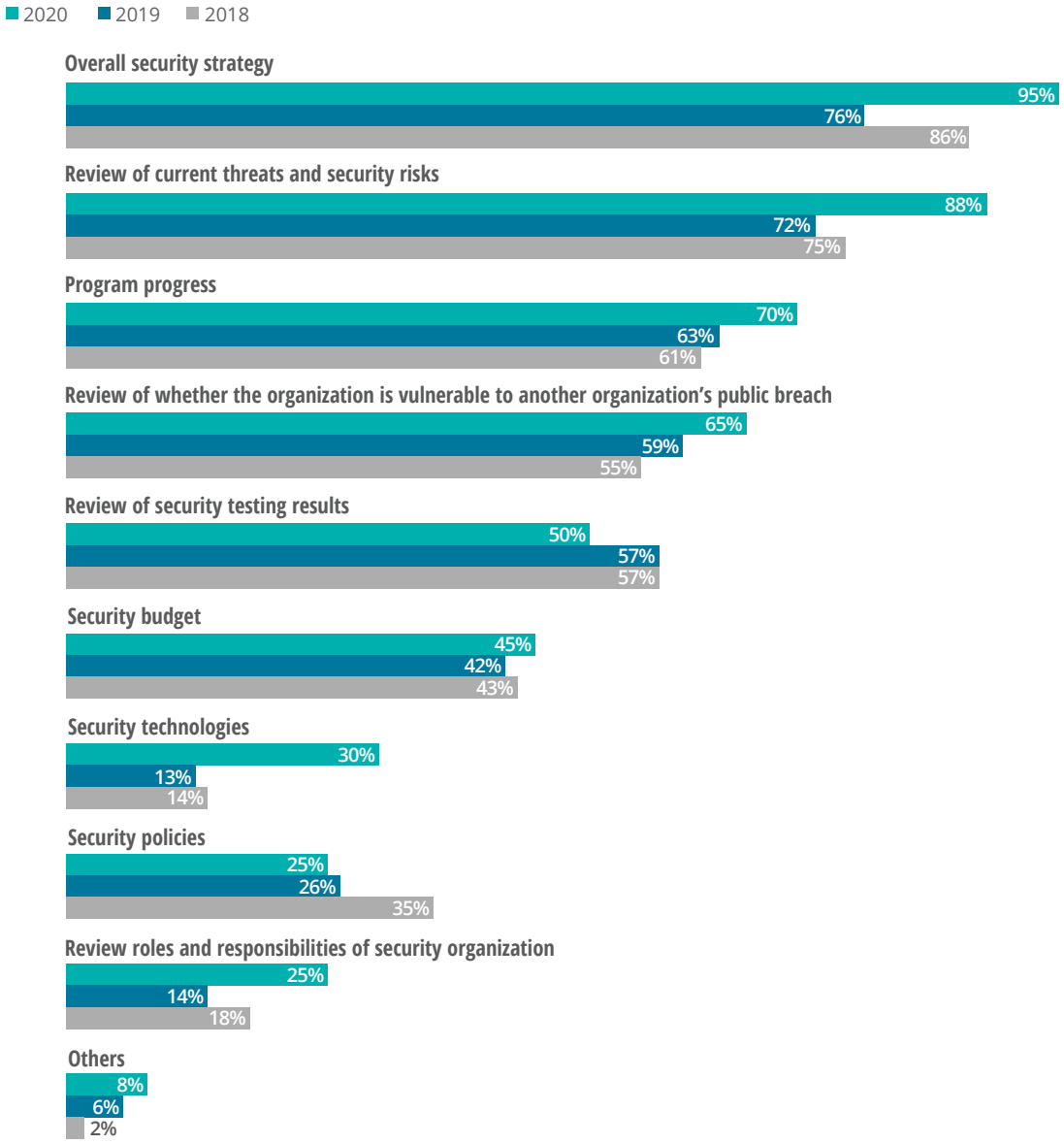
Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis.

Another reason for increased cybersecurity spending is increased pressure on boards and executive management teams, which has heightened their interest in cybersecurity at responding financial institutions (figure 4). Based on Deloitte's interactions with clients, CISOs who were able to continuously refine and articulate cybersecurity's value propositions to the board

FIGURE 4

Most cybersecurity areas saw more interest from the board and management teams

Top cybersecurity areas of interest for board/management identified by survey respondents



Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis.

tended to be more successful in securing board engagement.

Board engagement was not limited to strategic or operational areas. Security technologies rose from number nine among respondents in our prior survey to number seven in the most recent one, indicating that boards are becoming more interested in understanding the technical aspects of cybersecurity. Similarly, boards were more interested in reviewing roles and responsibilities of the security organization than in the past. This likely validates the growing emphasis around the notion that cybersecurity is everyone's job and not just the CISO's responsibility.

Survey respondents who rated their cyber programs as more mature had boards and management committees that were more interested in nearly all areas of cybersecurity than those from organizations with less mature cyber risk management programs. This underscores the importance of board engagement.

Looking ahead, given the tough macroeconomic conditions arising from the COVID-19 pandemic, many companies will likely be taking a hard look at whether they need to cut expenses across the board. Financial institutions, however, should be particularly judicious before making a reduction in cybersecurity budgets. Given the increased push toward digitization and the challenges raised by new, often remote work environments, as well as an increase in insider threats, cyber risks confronting most organizations are intensifying.[3]

Digital agendas shape cybersecurity programs at large financial institutions

TECHNOLOGY IS A part of everything that financial institutions do, but adopting new technologies across businesses comes with increased cyber risks. It is therefore likely no surprise that respondents ranked *rapid IT changes and rising complexities* as the No. 1 challenge in managing cybersecurity (figure 5) for the last three years, while the second biggest challenge was *the*

FIGURE 5

Challenges in managing cybersecurity

Respondents' top five challenges for large financial organizations

	2018	2019	2020
1	Rapid IT changes and rising complexities	Rapid IT changes and rising complexities	Rapid IT changes and rising complexities
2	Lack of skilled cyber professionals	Lack of skilled cyber professionals	Lack of skilled cyber professionals
3	Difficulty prioritizing options for securing the enterprise **tied with** inadequate functionality and interoperability of security solutions	Excessive focus on compliance with regulations; not enough focus on cyber risk management	Business growth and expansion
4	Excessive focus on compliance with regulations; not enough focus on cyber risk management	Business growth and expansion	Difficulty prioritizing options for securing the enterprise **tied with** inadequate functionality and interoperability of security solutions
5	Poor understanding of cyber risks and security	Difficulty prioritizing options for securing the enterprise	Difficulty prioritizing options for securing the enterprise

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis.

unavailability of skilled cyber professionals to help secure systems in such a rapidly evolving IT environment.

At the same time, *business growth and expansion*, a rising challenge according to respondents in our 2019 report, may recede for the time being, as companies have generally shifted focus from growth to pandemic response and recovery.

Top business issues and their security implications

More and more financial institutions are using emerging technologies to innovate and develop new products, services, and digital channels. But these critical enablers could become the target of additional cyberattacks. Thus, *embedding cybersecurity into new products and services* and *new channels* remain the top two business issues with security implications at large financial institutions surveyed (figure 6).

New products and services: Financial institutions today are often competing as well as collaborating with fintechs on product and service innovation. As companies strive to be first to market, these innovations often require speed and flexibility to be successful. However, companies should ensure that enough precautions are taken in designing, building, and utilizing new innovations, as new cybersecurity threats could emerge during any of these stages. The challenge for an organization's cybersecurity function is to create controls commensurate with the additional risk being taken on, without being perceived as a roadblock to innovation.

New channels: Companies often seek newer, easier ways to do business with customers, but newer channels may come with their own set of cyber vulnerabilities.

Take augmented or virtual reality (AR/VR), for example. Even as financial institutions experiment with using AR/VR to interact with clients, hackers

FIGURE 6

Embedding security into new products and services and new channels remain the top two business issues with security implications for large financial firms

Top three business issues with security implications for large FSI respondents

	2018	2019	2020
1	Embedding security into new products and services	Embedding security into new products and services	Embedding security into new products and services
2	New channels (digital, mobile)	New channels (digital, mobile)	New channels (digital, mobile)
3	New incumbents in the financial space	Cost reduction	Cost reduction

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis.

have devised sophisticated cyberattacks to compromise AR/VR applications and devices, which could potentially cause serious physical or financial damage. Traditional cybersecurity controls might not be well-suited to protect against these attacks.

Cybersecurity functions should assess the need to digitize and enhance their controls to adapt to and protect these new digital channels. Companies should also consider adopting "security-by-design" principles, where customized security controls are developed and embedded into the core structure of new channels as they are established and operationalized.

Cost reduction was already much on the minds of respondents, ranking third in each of the past two surveys, even before the fallout from COVID-19 became an additional concern.

However, going forward, cost reduction is likely to become more important in the post-COVID-19 world. Many companies will be under pressure to reduce expenses in a recovering economy, which could mean taking measures such as workforce restructuring, office space reductions due to the continuation of remote work for many employees, as well as increased use of automation or cloud capabilities, among other technology options.

Companies should consider corrective measures to ensure that cost-reduction initiatives do not expose them to additional cyber risks, such as insider threats.

However, actions taken to reduce operational costs should be evaluated carefully for their cybersecurity implications. Companies should consider corrective measures to ensure that cost-reduction initiatives do not expose them to additional cyber risks, such as insider threats.

CISOs will also likely be called upon to come up with recommendations to manage costs. They could consider using selective outsourcing or increasing automation, while supporting cost-reduction initiatives across the organization (for example, by enabling a secure migration of data and/or systems to the cloud).

Emerging technologies drive investment priorities for cybersecurity

For the past three years, *cloud* was consistently the No. 1 emerging technology in which respondents from large financial institutions said they wanted to invest (figure 7). Many of these companies already have a significant portion of their IT infrastructure in the cloud, with the next round of adoption being driven by the migration of core business applications. Many are also developing and deploying new apps for the digital world directly on the cloud.

At the same time, cloud service providers are augmenting their offerings through analytics-as-a-service and automation-as-a-service. Survey responses were in line with this trend: Most large firms expected to increase adoption of software-as-a-service and platform-as-a-service capabilities. However, with more data and applications moving outside the traditional security perimeter, the risk of cyberattacks increases.[4]

Data and analytics was the second emerging technology priority identified by large respondents. Since financial institutions have access to sensitive

FIGURE 7

Top digital priorities of large financial institutions surveyed are cloud, data/analytics, and automation

Top five emerging tech priorities for large FSI respondents

	2018	2019	2020
1	Cloud	Cloud	Cloud
2	Data/analytics	Data/analytics	Data/analytics
3	Mobile	Mobile	Artificial intelligence/cognitive computing
4	Artificial intelligence/cognitive Computing	Robotic process automation (RPA)	RPA
5	Social media	Artificial intelligence/cognitive computing	Mobile

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis

personal information, data breaches could have significant reputational implications. At the same time, many rely on insights from proprietary data and integration with third-party data vendors. Protecting data can be paramount to satisfying client data security and privacy expectations as well as meeting regulatory requirements.

Meanwhile, regulators have taken note of the large amounts of personal data captured and stored by companies, as well as their resiliency and data integrity. They have formed data protection standards, such as Europe's General Data Protection Regulation (GDPR),[5] and in the United States the Federal Financial Institutions Examination Council's Cybersecurity Profile[6] as well as the California Consumer Privacy Act.[7] These developments have made data protection an important focus area for cybersecurity.

With *artificial intelligence/cognitive* coming in third place and *robotic process automation* in fourth, it's clear that advanced automation and machine learning technologies present a new set of solutions that can help financial institutions transform operations and achieve cost reductions. While companies are likely taking precautions during development and training, these technologies are still evolving, with users slowly getting accustomed to working with robotic solutions (better known as bots). These bots have user privileges and can access sensitive company data and automated processing systems. This means hackers have a whole new attack surface

that can be leveraged to penetrate an organization's systems. Automation technology, despite its enormous potential, thus can add to a company's vulnerabilities during both development and training, as well as usage. Financial firms should address all of these potential issues.

Indeed, the increased focus of cybersecurity teams in protecting against vulnerabilities tied to emerging technology could be seen in the investment priorities of large financial institutions (figure 8).

People working in security have talked about identity and access management since the introduction of shared computing and mainframes. These remain a priority, albeit typically for different reasons. In an increasingly cloud-native and API-connected world, access control is once again a priority since these technologies expand identity and device proliferation, which creates additional identity types and new authentication requirements.[8] In an increasingly automated environment, this capability is also critical, and more complicated, in securing an organization.

Similarly, data security and protective technology can play a vital role in preventing data corruption and denial of service attacks.

The pace of digitization will likely only increase as the industry moves forward, and therefore should continue to be a key driver in influencing and prioritizing cybersecurity investments and capabilities. It is a leading practice to fully integrate cybersecurity functions into a company's digitization journey and to embed cybersecurity as a core consideration in transformation projects.

FIGURE 8

Emerging technologies are driving cybersecurity priorities for respondents

Top five NIST investment priorities for large FSI respondents

	2018	2019	2020
1	Security continuous monitoring	Protective technology	Access control
2	Access control	Access control	Protective technology
3	Anomalies and events	Anomalies and events	**Data security**
4	Detection processes	**Data security**	Detection processes
5	**Data security**	Detection processes	Anomalies and events

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis

Integrating cybersecurity with IT, while maintaining its strategic importance

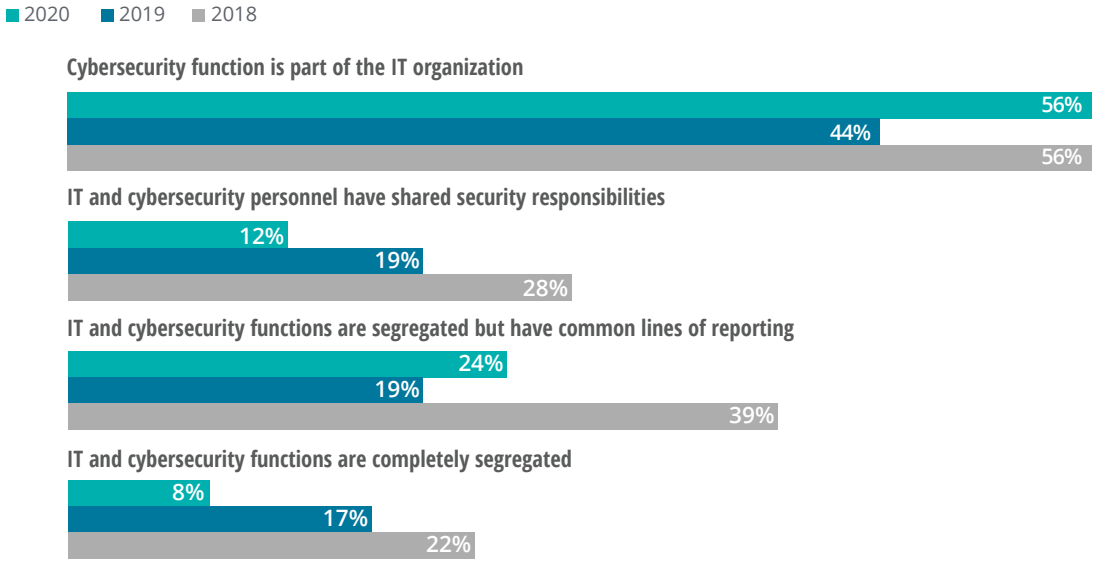
FINANCIAL COMPANIES MANAGE and operate cybersecurity programs in different ways, from how they are structured, to reporting lines, to establishing focus areas for cybersecurity spending. Many have adopted a mix-and-match approach based on their company's objectives.

In this dynamic environment, many financial firms are now closely linking cybersecurity programs to technology initiatives to effectively mitigate emerging cyber risks. This was reflected in the way cyber risk management was organized at large financial institutions participating in the survey. Indeed, a majority of respondents cited cybersecurity as a part of their IT organization (figure 9).

FIGURE 9

More than half of large financial respondents from large firms had cybersecurity as a part of their IT organization

Cybersecurity integration with IT for large FSI respondents

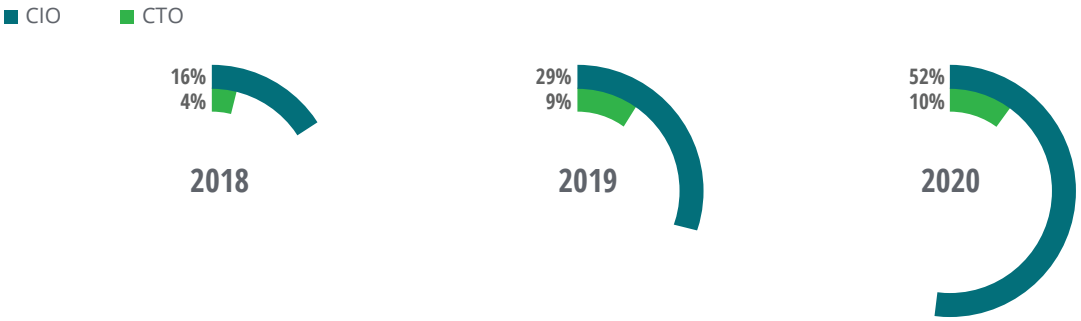


Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis

FIGURE 10

More than half of CISOs reported to CIO/CTOs, reflecting the close alignment necessary between cybersecurity and IT goals

Percentage of CISOs surveyed reporting to the CIO or CTO at large firms



Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis.

The close alignment between cybersecurity and IT goals was also reflected in the reporting structure for survey respondents. Among CISOs surveyed from large financial firms, 62% report either to the chief information officer (CIO) or the chief technology officer (CTO), a substantial jump from 38% the year before and only 20% the year before that (figure 10).

By closely aligning cybersecurity with the IT function, financial institutions can be better positioned to deal with emerging cyber risks in a faster and more effective manner, helping their IT partners become more agile.

While the first line of defense in cybersecurity is often aligned closely to technology functions through common lines of reporting, security personnel usually have clearly segregated roles and responsibilities. In second lines of defense, however, cybersecurity is often a part of the technology or risk functions without clearly delineated requirements, roles, or responsibilities.

Companies should therefore clearly delineate cybersecurity from technology or risk functions across both the first and second lines of defense by providing clear separation of roles and responsibilities.

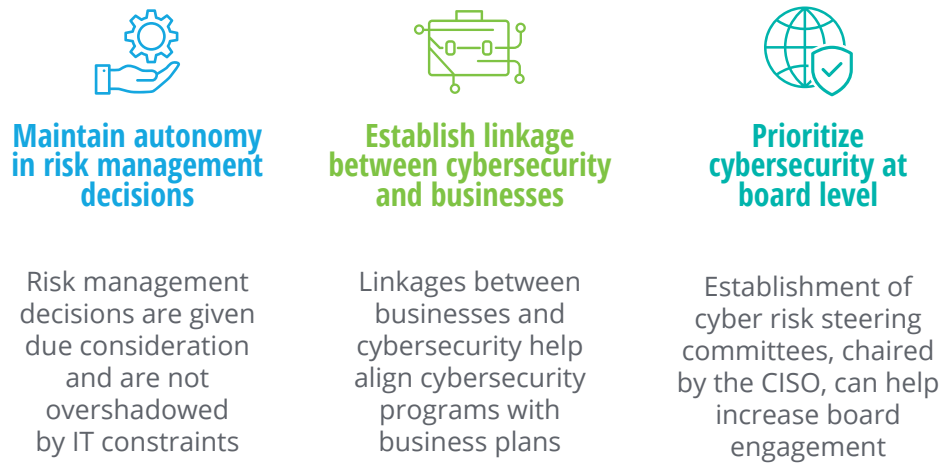
Maintaining the strategic importance of cybersecurity

Cyberthreats and attacks are no longer just a technology risk, but a business risk as well.[9] That's why the cybersecurity function should have sufficient independence and prominence. This can help ensure that decisions related to risk management are given due consideration and are not influenced or overshadowed by other IT considerations or constraints.

If cybersecurity is part of IT, it may not have enough visibility and ties to actual lines of business. At the same time, with CISOs reporting to CIOs,

FIGURE 11

How might cybersecurity retain independence within IT?



Source: Deloitte Center for Financial Services analysis.

other stakeholder relationships may matter even more to balance risk and business priorities.

Companies should therefore consider specific measures to create linkages among lines of business, risk partners, and cybersecurity. This can be accomplished by creating steering committees, hiring business information security officers (BISOs), and other options. These actions could also help align cybersecurity with future business plans (figure 11).

Finally, companies should work on ensuring that boards and management committees place cybersecurity high on their agendas. As noted earlier, having an engaged board can help the entire organization focus on the challenge of managing cyber risk while assuring that adequate resources are allocated. And board oversight should be ongoing, rather than only at the initial stages or when there is a cyber incident.

The way forward

THE COVID-19 PANDEMIC has significantly disrupted financial institutions and the ways they operate globally. Remote work has increased significantly, and—as a result—the use of videoconferencing and team collaboration applications has skyrocketed. And these changes may not disappear as firms recover. Indeed, a recent Deloitte report found that many financial institutions are evaluating permanent remote work for at least part of their workforce. Based on conversations with industry leaders, some companies are considering remote work for 30% or more of their employees on a more permanent basis.[10]

Cybersecurity organizations will need to quickly adapt to this new operating environment by implementing enhanced controls and endpoint protection technologies to exert greater control over end-user devices. Companies should consider increasing training and awareness activities, focusing on remote etiquette for work-from-home environments.

At the same time, with lines blurring among employees, customers, contractors, and partners/vendors in general, firms should consider implementing "zero trust" principles for access since the organization's perimeter is essentially gone. This means every transaction involving flow of data, whether it be through networks, applications, users, devices, or workloads, is controlled for least privileged access.

Companies should also digitally enable their cyber function to improve agility and automation. Weaving security-by-design principles into IT service development and embedding cybersecurity requirements into the architecture and design stages of the software development life cycle could help companies get ahead of evolving threats.

That said, CISOs should not take their eyes off longer-term goals, which likely include aligning with the company's strategic priorities, managing talent challenges, and addressing external issues such as regulation. Such broad engagement can highlight the value cybersecurity adds to the

FIGURE 12

Maintaining the business value of cybersecurity

Source: Deloitte Center for Financial Services analysis.

business (figure 12). To execute on this well, stakeholder engagement will likely become critical, regardless of the operating model used.

Demonstrating the business value of cybersecurity

Effective cybersecurity programs should demonstrate business value. To help ensure the value of cybersecurity is fully realized and appreciated by top management, CISOs can focus on several actions, including:

1. Align with company focus

- CISOs should enhance and implement cybersecurity capabilities to support the broader business and technology strategies and objectives of the organization.
- When companies implement cost-reduction activities, cybersecurity teams should support the organization by implementing required cybersecurity controls.
- Security teams should support activities beyond cyber resilience (such as business continuity planning and disaster recovery), with an emphasis on enabling operational resilience.
- The cybersecurity function should support outsourcing strategies and help choose third parties that present better resilience capabilities and can meet consistent service levels.

2. Address external considerations

- Regulatory requirements are likely to concentrate more on boosting resilience through activities such as onsite assessment requirements for third parties.
- Depending on the international response to the pandemic, there could be increased geopolitical risk that might impact both global execution as well as the threat environment. This will likely require security teams to be ready to quickly adapt to fast-changing scenarios.
- The volume and velocity of the threat environment was increasing rapidly even before the COVID-19 outbreak. CISOs could add increased automation and orchestration at security operations centers and ensure it does not drain valuable CISO or executive time.

3. Focus on supporting talent

- While talent shortages have been a perennial challenge, other factors are likely to become important as the world recovers from the pandemic, such as team members' health, remote work arrangements, and physical design of office spaces—including security operations centers and conference rooms.
- CISOs should reduce dependence on select individuals who have exclusive knowledge of tools or processes by cross training team members.
- CISOs and their leadership teams should try to build and uphold a positive, dynamic work culture in their cyber organizations. This could be crucial in attracting and retaining the best talent.

While the challenges presented by the current operating environment are vast, CISOs should stay focused on broader, longer-term organizational objectives and plans. This can help ensure cybersecurity is prepared to keep up with the transformative changes that lie ahead.

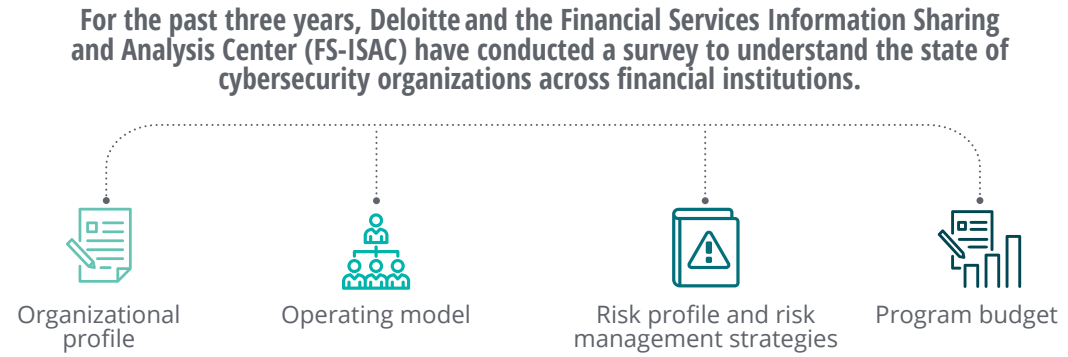
About the survey

This article is based on surveys fielded in each of the last three years by the Financial Services Information Sharing and Analysis Center (FS-ISAC) of its members, all CISOs or their equivalents, in conjunction with the Cyber & Strategic Risk Services practice of Deloitte & Touche LLP. The most recent survey was launched in late 2019 and concluded on January 27, 2020. The survey results are identified and presented according to the year of their publication—2020 for the most recent, preceded by 2019 and 2018.

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, budgets, the level of board interest in the CISO's work, as well as which cybersecurity capability areas were prioritized in terms of spending (figure 13).

FIGURE 13

Cybersecurity program aspects covered in the survey



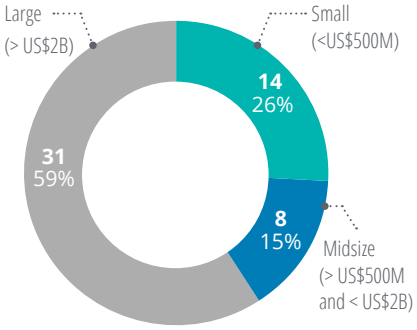
Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2018, 2019, and 2020; Deloitte Center for Financial Services analysis.

This report provides an analysis of responses across all three years the survey was conducted to spot cyber risk trends across the industry.

Fifty-three companies participated, with representation across multiple revenue levels (figure 14) and all sectors (figure 15, adding up to more than 53 because some respondents represented multiple categories). In addition, some or all of the respondents may have been different for each of the surveys.

FIGURE14

Respondent organizations, by revenue

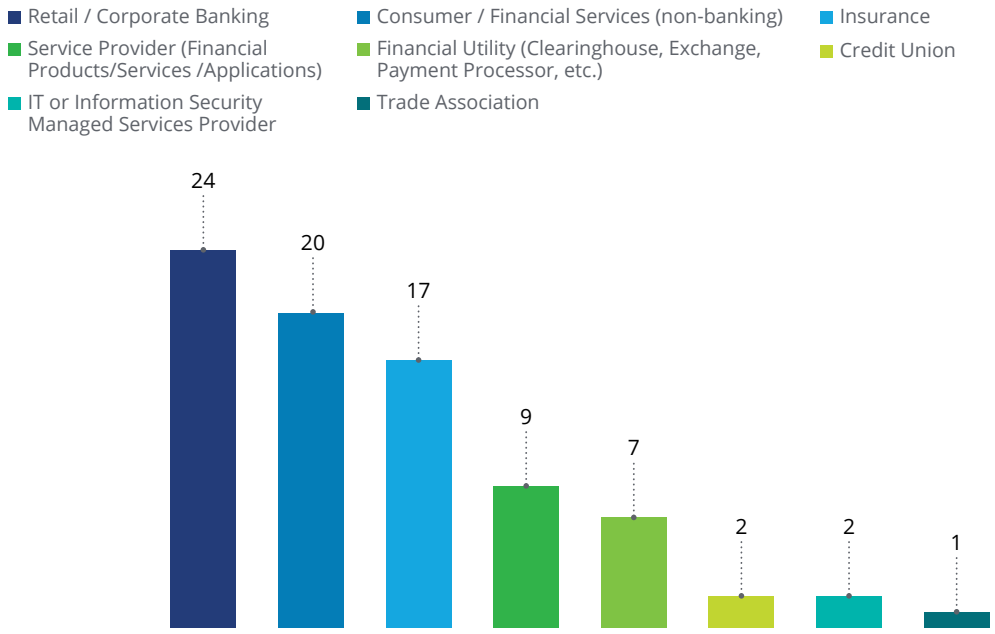


Notes: Large includes large (>US$2B and <US$5B); giant: (>US$5B and <US$30B); and super giant: (>US$30B).

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey report, 2020; Deloitte Center for Financial Services analysis.

FIGURE 15

Respondent organizations, by financial sector



Note: Respondents could select more than one option.

Sources: 2020 FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey report, Deloitte Center for Financial Services analysis.

Endnotes

1. Peter Baldwin, "New York Department of Financial Services issues new guidance regarding COVID-19 cybersecurity risks," *National Law Review* 10, no. 176 (2020).
2. Iman Ghosh, "This is the crippling cost of cybercrime on corporations," World Economic Forum, November 7, 2019.
3. Deloitte, "COVID-19 executive cyber briefing: Read the latest," May 20, 2020.
4. Aaron Brown and Mark Campbell, *Cloud cyber risk management: Managing cyber risks on the journey to Amazon Web Services (AWS) solutions*, Deloitte, 2017.
5. Andrew Rossow, "The birth of GDPR: What it is and what you need to know," *Forbes*, May 25, 2018.
6. Dave Kovaleski, "FFIEC backs Cybersecurity Profile tool for *financial institutions," Financial Regulation News*, August 30, 2019.
7. Devon Coldewey, "The California Consumer Privacy Act officially takes effect today," *TechCrunch*, January 1, 2020.
8. Aaron Brown et al., *Cloud and identity and access management: How to do identity and access management in Amazon Web Services*, Deloitte, 2019.
9. Tommy Viljoen, *Cybercrime is not just a tech problem*, Deloitte, accessed June 24, 2020.
10. Francisco J. Acoba, Darin Buelow, and Tina Witney, *COVID-19 return-to-the-workplace strategies: Emerging lessons and key questions for financial services leaders*, Deloitte Insights, May 15, 2020.

Acknowledgments

Coauthor **Nikhil Gokhale** wishes to thank **Meghana Rajiv Kanitkar**, **Sriram Balakrishnan**, **Prachi Ashani, Sanjay Vadrevu, Surya Kiran Sharma**, **Yashvardhan Kabra**, and the many others who provided insights and perspectives in the development of this report. The authors also thank the **Financial Services Information Sharing and Analysis Center (FS-ISAC)** for their help in fielding and analyzing this survey.

About the authors

Julie Bernard | juliebernard@deloitte.com

Julie Bernard is a principal with Deloitte Risk & Financial Advisory and is the US banking and capital markets leader for Cyber & Strategic Risk Services at Deloitte & Touche LLP. She has more than 25 years of experience serving the world's top financial institutions at the intersection between business process and information technology. With an extensive background in security strategy, privacy, consumer authentication, fraud prevention, and threat management, she helps clients be more secure, vigilant, and resilient in the face of an ever-increasing array of cyber threats and technology complexity. She is a past board member of the Executive Women's Forum and currently sits on the Advisory Board for the Financial Services Information Sharing and Analysis Center (FS-ISAC). She earned her BA in music and business administration at Westminster College and an MBA in finance at Rensselaer Polytechnic Institute.

Deborah Golden | debgolden@deloitte.com

Deborah Golden is a principal at Deloitte & Touche LLP, is the US Cyber & Strategic Risk leader for Deloitte Risk & Financial Advisory. In the prior six years, Golden served as the Government & Public Services (GPS) Cyber Risk Services leader, as well as the GPS Advisory Market Offering leader, GPS Empowered Well-Being leader and the lead principal for a major federal government health care provider. Golden has more than 25 years of information technology experience spanning numerous industries, with an in-depth focus on government and public services, life sciences and health care, and financial services. She specializes in collaborating with clients on cybersecurity and technology transformation, and privacy and governance initiatives.

Mark Nicholson | manicholson@deloitte.com

Mark Nicholson is a principal at Deloitte & Touche LLP, is the Cyber & Strategic Risk Services Financial Services industry leader for Deloitte Risk & Financial Advisory. Nicholson helps complex organizations more confidently leverage advanced technologies to build cyber risk programs that better align security investments with risk priorities, establish improved threat awareness and visibility, and helps them strengthen their ability to thrive in the face of cyber incidents.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Julie Bernard
Principal | Deloitte Risk & Financial Advisory | Cyber & Strategic Risk Services | Deloitte & Touche LLP
+ 1 704 227 7851 | juliebernard@deloitte.com

Deborah Golden
Principal | Deloitte Risk & Financial Advisory | Cyber & Strategic Risk Services | Deloitte & Touche LLP
+1 571 882 5106 | debgolden@deloitte.com

Mark Nicholson
Principal | Deloitte Risk & Financial Advisory | Cyber & Strategic Risk Services | Deloitte & Touche LLP
+1 201 499 0586 | manicholson@deloitte.com

Steven Silberstein
CEO | FS-ISAC
+1 877 612 2622 | ssilberstein@fsisac.com

The 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
Senior manager | Deloitte Center for Financial Services | Deloitte Services LP
+ 1 212 436 5521| samfriedman@deloitte.com

FS-ISAC

Ray Irving
Managing director | Global Business Services
+41 76 303 50 70 | rirving@fsisac.com

Brian Hansen
Executive director | Asia Pacific
+65 9165 5931| bhansen@fsisac.com

Deloitte Cyber & Strategic Risk Services

Cyber is enterprisewide. So are our services. With human insight, technological innovation, and enterprisewide cyber solutions, Deloitte Cyber will work alongside you to help you find answers and solve for the complexity of each challenge, from the boardroom to the factory floor. Learn more.

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

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Karen Edelman, Hannah Bachman, Nairita Gangopadhyay, and Rupesh Bhat

Creative: Sonya Vasilieff and Tushar Barman

Promotion: Ankana Chakraborty

Cover artwork: Rocco Baviera

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