Deloitte.

Cybersecurity in a post-pandemic world:

A focus on financial services

Contents

Executive summary

How the shift toward **remote workforces** and **virtual customer engagement** fuelled **digitalization** and changed the cybersecurity landscape in financial services.

- Two out of three surveyed[1] have experienced between one and 10 cyber incidents or breaches between 2020 and 2021. It only takes one incident to potentially cripple an organization and bring reputational, financial, or operational havoc.
- The rapid growth of remote work has increased the number of challenges organizations face in securing their ecosystem. Imagine going from one managed network to managing hundreds of networks, depending on the size of your remote staff.
- It is time to retire legacy systems to pave the way for the latest tools and technologies in order to provide effective online and mobile services and differentiate yourself in the marketplace.
- Data privacy and security, and the struggle to attract talent, remain critical reasons[2] for the hesitation to mature core IT infrastructures to cloud technologies.
- CISOs should be given greater authority to influence the lines of business and gather information from across the enterprise. They need to be ready to have open and frank conversations with board members, senior management, and stakeholders.
- The rush toward creating new fintech solutions has coincided with a marked rise in cyber-attacks. In fact, attacks targeting financial apps rose by 38% year-over-year.[3]
- Extended enterprise risk is a harsh reality that organizations need to plan around. Dependency on third, fourth, and fifth parties will likely continue to increase, increasing the need to monitor real-time.
- Human vulnerability remains the No. 1 cybersecurity threat. Awareness training remains a priority but is not sufficient. Creating a culture of cybersecurity is important.
- CEOs and boards are increasingly calling for more sophisticated risk quantification techniques that tie into broader business risks.

New risks compel new responses

As the COVID-19 pandemic pushed some workforces to go fully remote, and customers demanded almost-complete virtual engagement, financial services leaders had to find ways to digitalize their operational, distribution, and customer engagement processes. Meanwhile, cyber risk professionals were simultaneously faced with the enormous challenge of rapidly adapting their cybersecurity capabilities in response to the evolving digitalization needs.

While the pandemic may someday relent, hybrid work and digitalization are certainly here to stay, requiring financial services organizations to assess how these adaptations should mature for the long term. The industry appears to be committing to this intention by stepping up cyber defense efforts. However, work remains to be done to position for the future by prioritizing the digital transformation agenda, securing modernization activities, and building resilient digital operations.

To better understand how organizations are responding to these emerging pressures, Deloitte Touche Tohmatsu Limited (DTTL) surveyed nearly 600 C-suite executives globally across several industries.[4] This report focuses exclusively on the 162 responses received from financial services organizations, encompassing those in the banking and capital markets, insurance, investment management, and real estate sectors. Our analysis led to four definitive conclusions that financial services leaders can use to help structure their cybersecurity programs, identify investment priorities, and allocate budgets:

- Short-term fixes should advance immediately to steady state
- Legacy systems are slated for retirement
- Extended ecosystems call for stronger detection and control mechanisms
- Some things never change

In the remainder of this paper, we explore each of these conclusions in greater detail.

Short-term fixes should advance promptly to steady state

The pandemic forced financial services IT organizations to roll out programs on an expedited basis to support remote workforces and enable their business lines to provide digital-first products and services. Given the pace of these changes, many of these programs have been languishing in "test or pilot mode" as organizations scrambled to adapt to radically different employee and customer engagement models.

Now that hybrid workforces and virtual engagement are here to stay, the time for testing is over—and the work begins to determine which changes to incorporate for the long term and which challenges remain to be resolved.

Cause for concern

If evidence is needed to analyze the need to move to a new steady state, it is ready at hand. Over the past year, cyber incidents have ballooned. According to the Identity Theft Resource Center, data breaches rose 17% between 2020 and 2021.[5] And 67% of survey respondents report that their organizations experienced between one and 10 cyber incidents or breaches over the past year—and an additional 15% say they experienced 11 to 15 incidents.

DTTL's 2021 Future of Cyber Survey supported these findings. The increase in remote work has introduced increased complexities in data management and perimeter protection, resulting as the biggest challenges impacting the financial services industry (figure 1).

This contrasts with the past several years, where rapid technology change was identified as the No. 1 challenge in managing cybersecurity.[6]

A rallying call

Survey respondents highlighted several potential causes for increased cyber incidents, including insufficient incident detection and response capabilities, network and endpoint assets that are too complex to protect, failure to properly identify risks, unclear governance and ownership of cyber topics, and employee failure to follow cybersecurity policies.

Firms have traditionally used endpoint detection and response (EDR) and security monitoring to help detect cyber-threats. But greater controls will be required as new operating models emerge. This includes aggressively monitoring access controls and instituting a continuous cycle of employee awareness training and compliance tracking—both for staff returning to the office and for those who plan to continue working remotely.

Figure 1: What are the biggest challenges in managing cybersecurity across your organization?

	All Financial Services	Banking & Capital Markets	Insurance	Investment Mgmt.	Real Estate
Increase of data management/ perimeter, and complexities	1	1	1	1	1
Better prioritization of cyber risk across the enterprise	2	4	3	2	2
Inability to match rapid technology changes	3	2	2	3	5
Lack of skilled cyber professionals	4	3	6	6	2
Inadequate governance	5	5	4	4	4

Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

Legacy systems are slated for retirement

While cybersecurity has gained higher visibility among boards and regulators alike, it's time for IT teams to further mature their infrastructures as the industry as a whole aligns behind efforts to provide effective online and mobile services and virtualize the workforce.

On the plus side, much of the required digital ecosystem was already in place to scale up rapidly. Despite having laid this foundation, our survey[7] shows that financial services organizations (and particularly large enterprises) are still early in their adoption of cloud technologies.

Maturing core infrastructure

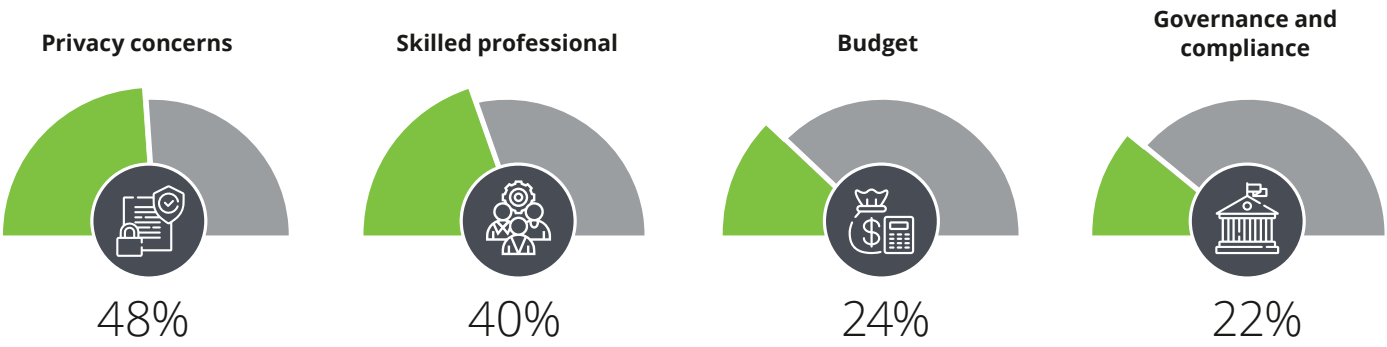
Part of the hesitance to embark on the transformation journey can be traced to ongoing concerns around full-scale adoption of cloud technologies, with respondents citing privacy and the struggle to attract talent as specific concerns (figure 2).

Similarly, financial services respondents also said the visibility of the cloud environment and compliance were top of mind in their efforts to protect cloud applications and workloads (figure 3).

Firms should therefore assess the cloud-readiness of controls, especially since they need to meet expected control objectives and build controls applicable to the cloud at a time when many are barely keeping up with existing requirements. This imperative is further complicated by the fact that traditional security management practices frequently can't keep pace with digital transformation agendas—resulting in control gaps, compliance missteps, and heightened security risks.

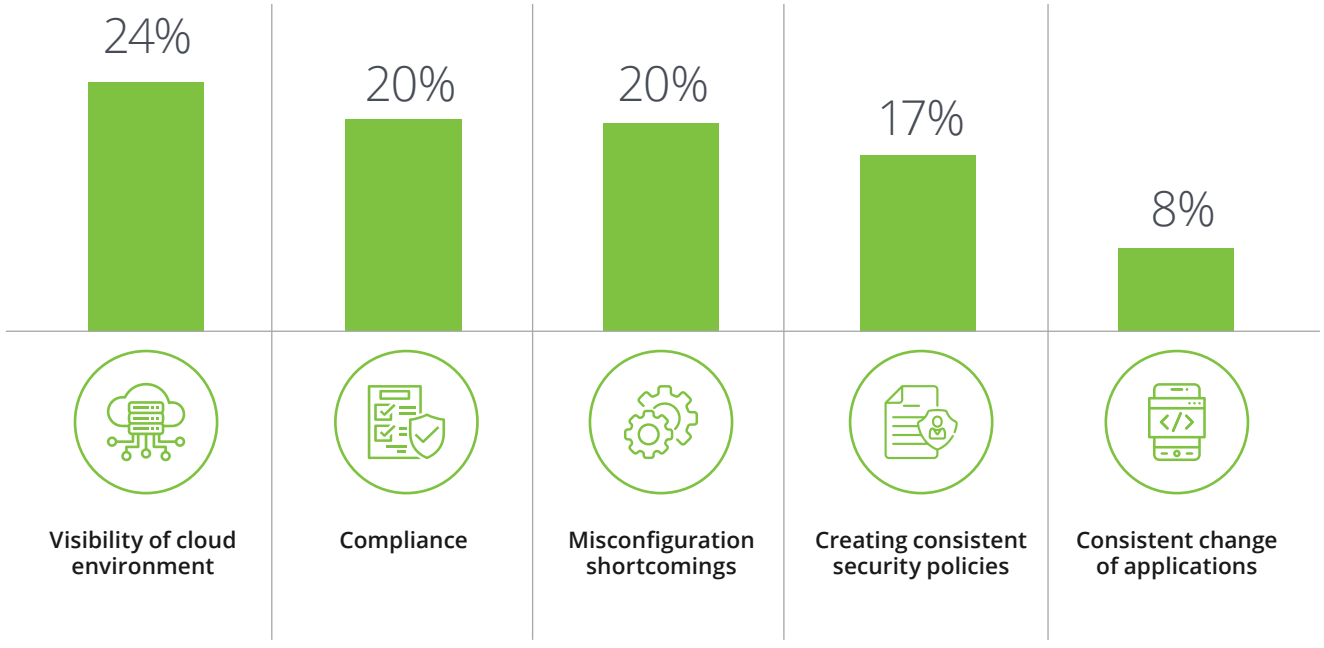
Mitigating these challenges calls for enhanced coordination across the business units, the automation of controls and control testing, and improved capacity to assess a broader range of potential risks—from expanded attack surfaces to third-party risks to functional maturity.

Figure 2: What type of investments or requirements are influencing your commitment to security in the cloud?

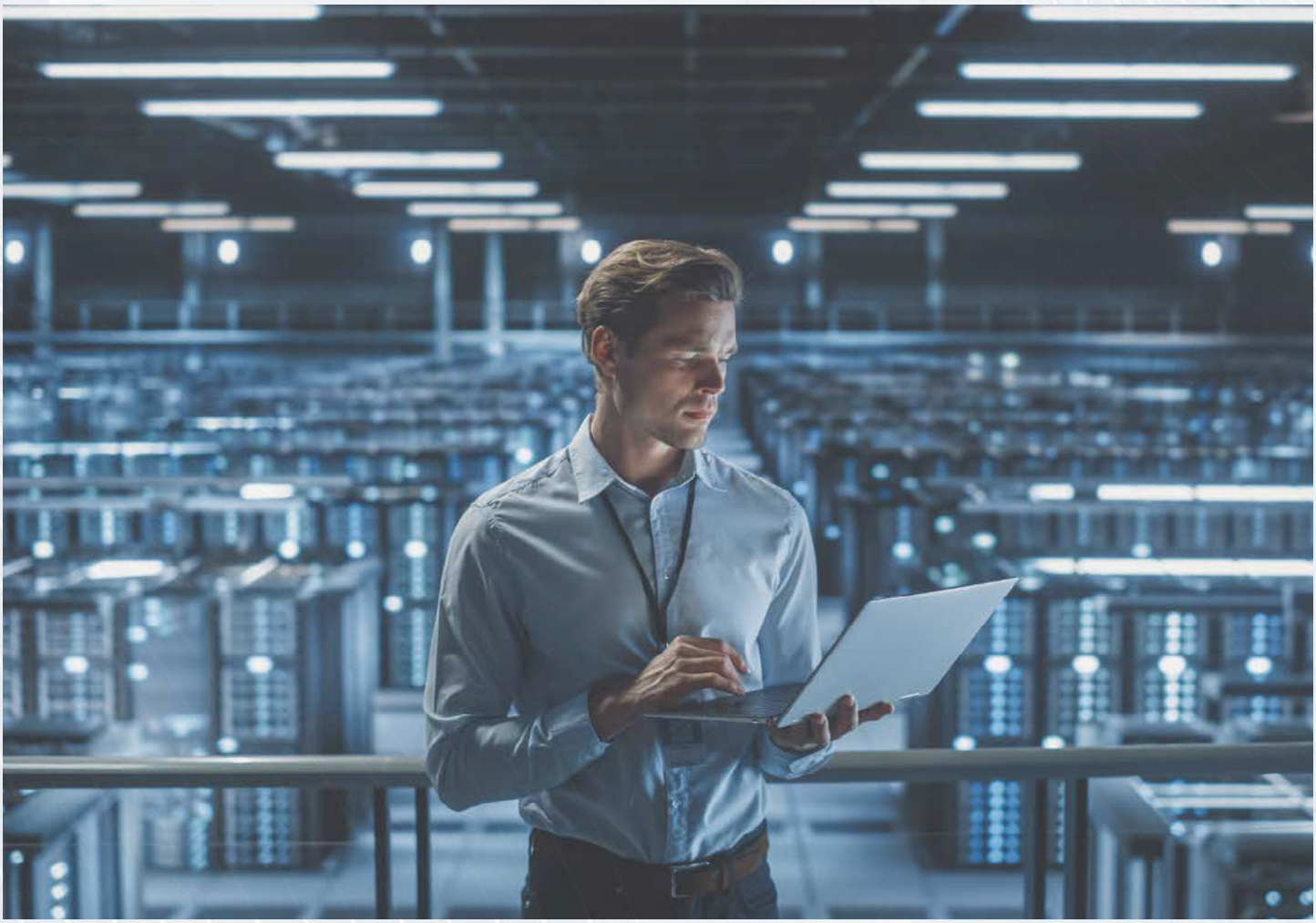


Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

Figure 3: What is the biggest "weight on your shoulders" when protecting cloud applications or workloads?



Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

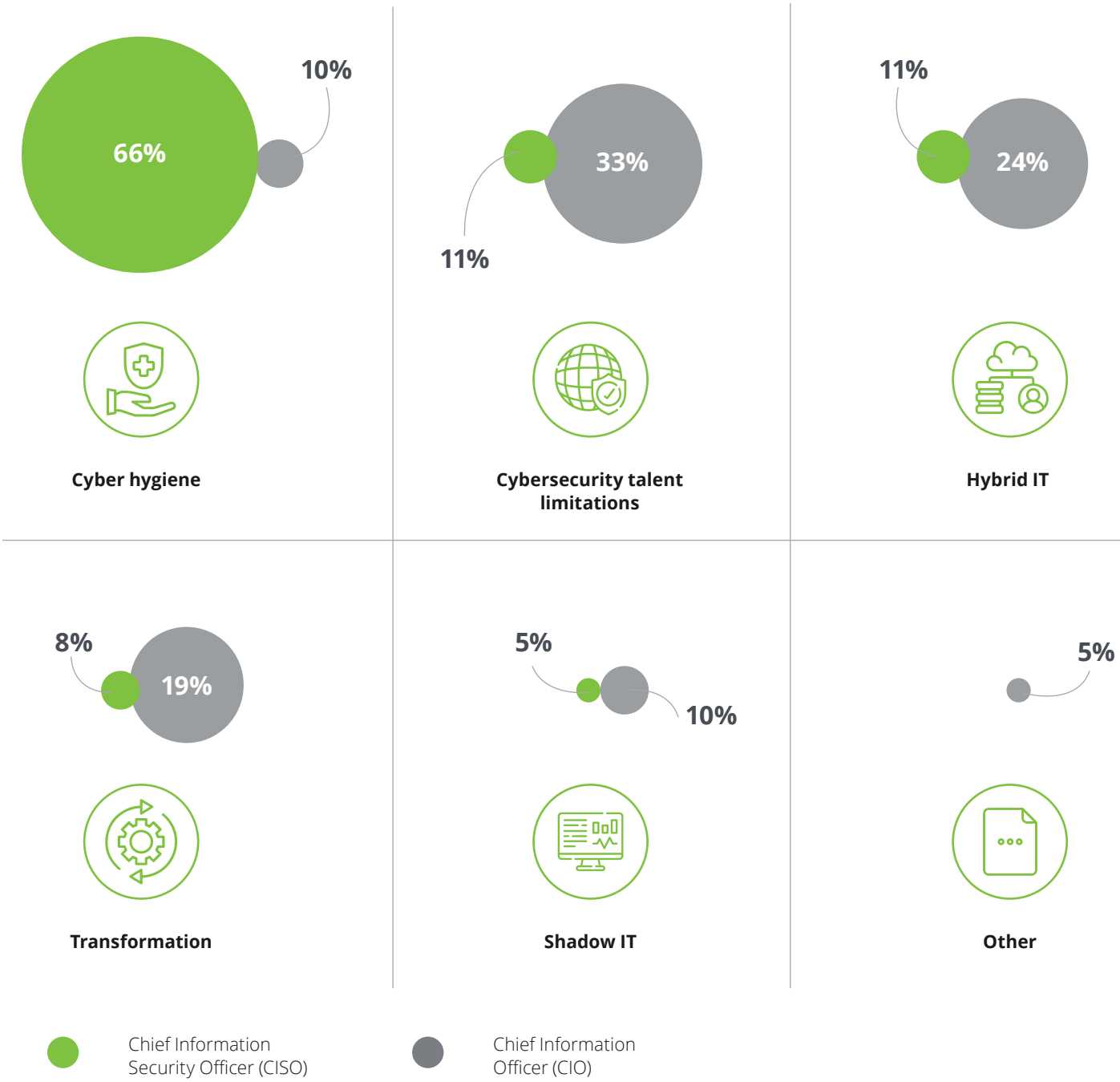


Maturing cyber infrastructure

Looking beyond core systems, financial services organizations should also consider revamping their legacy cybersecurity infrastructure. According to the survey[8], scaled cyber solutions both ***in*** the cloud and ***for*** the cloud are being prioritized as financial services organizations try to enhance their cyber defense capabilities. For instance, 31% of surveyed financial services organizations say they are choosing cloud-based Identity-as-a-Service (IDaaS) solutions, with in-house contractors preferred to procure, implement, and provide ongoing delivery of identity capabilities.

But organizational priorities appear to vary among leadership. While 66% of responding chief information security officers (CISOs) identify cyber hygiene (including IT asset management, configuration management, and patch and vulnerability management) as the most challenging aspect of cybersecurity management across the organization, 33% of chief information officers (CIOs) think cyber talent limitations are the real challenge, along with hybrid IT and transformation (figure 4).

Figure 4: Which of the following is the most challenging aspect of cybersecurity management across your organization's infrastructure?



Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

To help resolve some of these tensions, CISOs likely need greater authority to influence the lines of business, gather information from across the enterprise, and communicate directly with the board and senior leaders. But this imperative appears to vary depending on organizational size. Among the largest financial services organizations surveyed, defined as those with more than $30 billion in revenue, 28% say their boards address cybersecurity issues monthly, while at mid-sized organizations ($500 million - $5 billion in revenue) cybersecurity only makes it onto the monthly board agenda 10% of the time (figure 5).

Nevertheless, it's clear that cybersecurity has firmly captured board attention. If CISOs and cybersecurity teams aim to sustain this board-level visibility, they need to find ways to integrate cybersecurity into product design and platform innovation from the outset.

With cyber risks permeating everywhere from customer touchpoints to remote employee devices, IT departments can no longer operate in silos and CISOs should look well beyond network functionality. Instead, they should be ready to talk to board members, senior management, and stakeholders across the three lines of defense, etc.—in language they understand—about the cyber risks that most concern them.

Based on the survey responses, it seems CISOs remain focused on cyber hygiene, talent limitations, and hybrid IT (which refers to technology that supports in-house traditional infrastructure and public cloud infrastructure in parallel)—issues that remain unaddressed as cybersecurity professionals continue to get sidetracked simply plugging holes and remediating vulnerabilities in their existing infrastructure. To mitigate evolving cyber risks, CISOs should determine how to broaden their focus to execute on more strategic development, security, and operations (DevSecOps) initiatives.

Figure 5: How often is cybersecurity on your board's agenda?

Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

Extended ecosystems call for stronger detection and controls mechanisms

Although third-party risk management has been a regulatory requirement for years, accelerating trends—such as open banking and fintech relationships—are simply amplifying this mandate. As a case in point, a Deloitte Center for Financial Services survey[9] found that one in five US consumers considers open banking valuable, with interest especially high among millennials and Gen Z. And relationships between traditional financial services organizations and fintechs have already shifted how financial services are structured, delivered, and consumed, resulting in both unprecedented disruption and boundless innovation.

Yet, despite the clear upside, security vulnerabilities remain. The constant development of new open application programming interfaces (APIs) to connect banks with other institutions has sparked debate about who owns a customer's financial data. And the rush toward creating new fintech solutions has coincided with a marked rise in cyber-attacks. In the first six months of 2021 alone, attacks targeting financial apps rose by 38% year-over-year.[10]

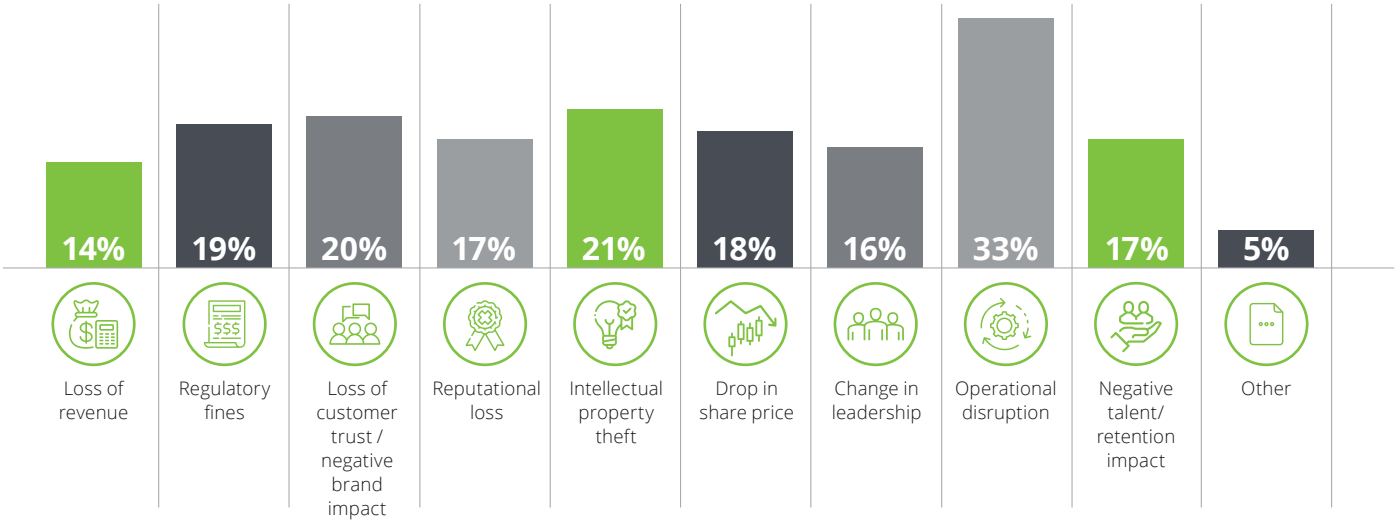
As a result, cybersecurity professionals are under greater pressure to protect their increasingly partner-oriented and virtual enterprises. Indeed, extended enterprise control deficiencies are now considered by survey respondents to be the second-highest threat at many financial services organizations, up from the No. 3 spot last year.[11]

In this context, the "extended enterprise" refers to the extended ecosystem of third-party vendors, suppliers, agents, brokers, and partners that support financial services organizations and/or their customers—such as technology solution providers, payment processors, clearing houses, and beyond.

The impact of cyber incidents

The extended enterprise may also open the organization up to additional cyber incidents. When asked about cyber incidents and breaches, survey respondents[12] indicated that operational disruption caused the biggest impact (figure 6).

Figure 6: What were the biggest impacts of cyber incidents or breaches on your organization? (Please select up to 2 answers)



Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

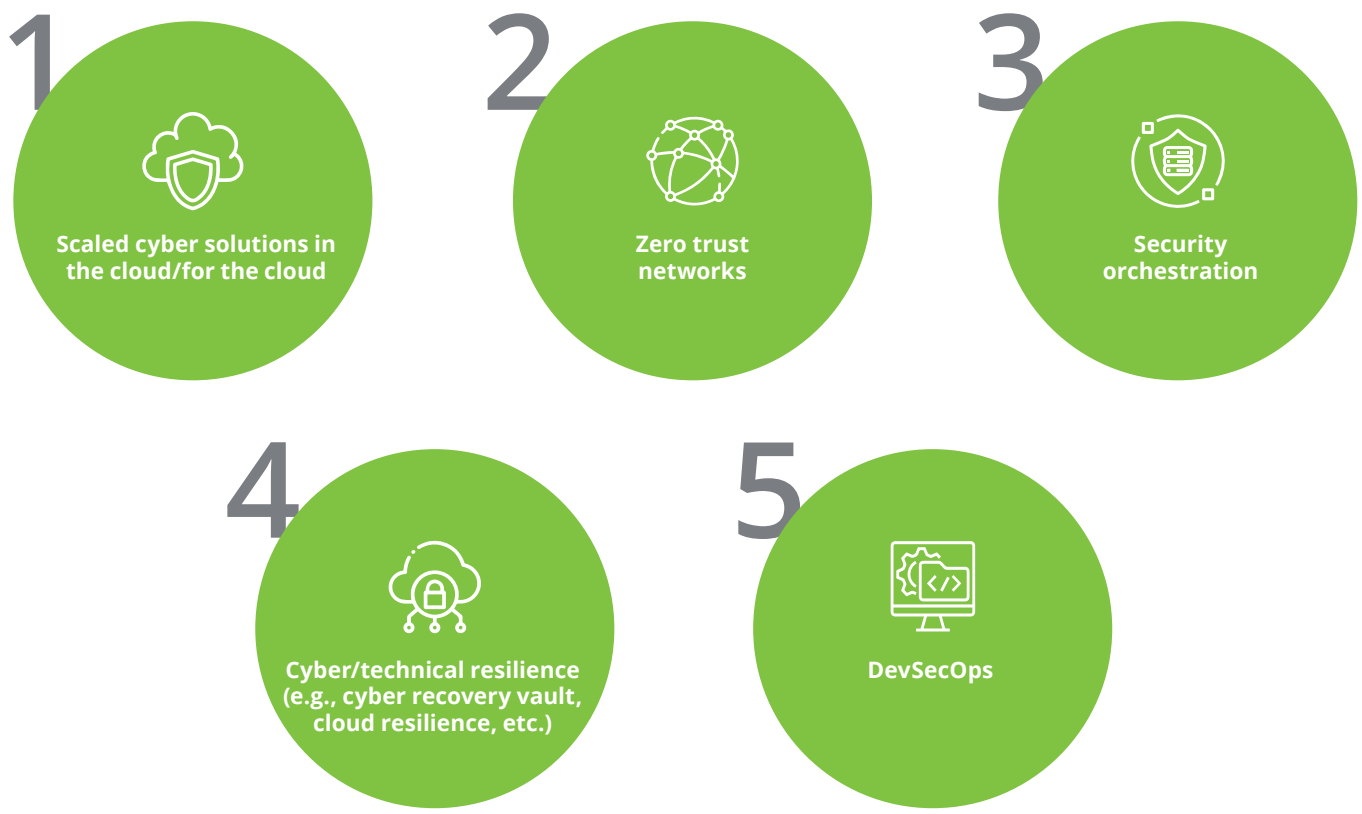
Strengthening the control environment

With extended enterprise gaining ground, zero trust continues to emerge as an essential practice for enforcing least privileged access to everything from networks and applications to users, devices, and workloads.

Unlike a technology or single solution, zero trust is a set of policies based on the principle of "never trust, always verify," where a traditional perimeter-based (or "castle and moat") approach of security management shifts to one where trust is established between individual resources and consumers as and when required. The aim is to create trusted connections that hinge on a set of internal and external factors that are constantly revalidated.

Hearteningly, respondents seem to be prioritizing the adoption of zero trust frameworks, along with cyber defenses such as automation and security orchestration (figure 7). Going forward, financial services organizations should also look at further digitalizing their cyber functions to improve agility and speed. Weaving security-by-design principles into IT service development and embedding cybersecurity requirements into the architecture and design stages of the software development lifecycle could help organizations get ahead of evolving threats.

Figure 7: Which of the following cyber defense concepts are being prioritized / invested in to transform your security capabilities?



Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

Some things never change

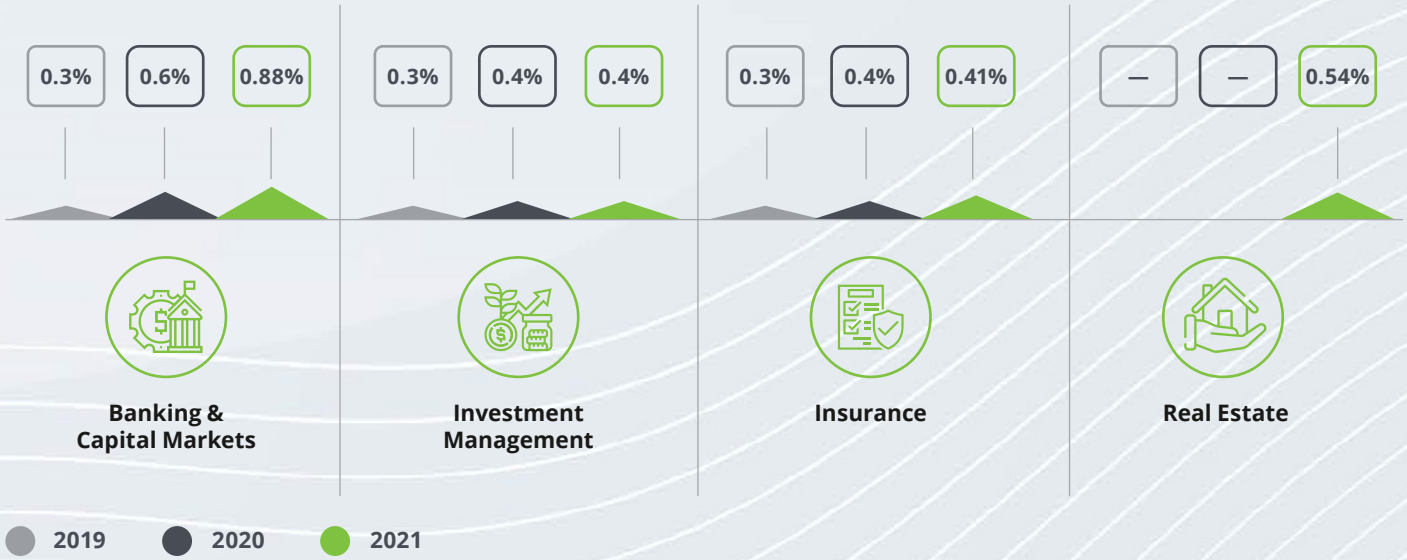
Despite this more dynamic environment, our survey[13] also highlighted two evergreen topics: the willingness to fund cyber risk management, and the inability of employees to follow common sense risk management protocols.

In the first case, budgets for cybersecurity initiatives remain broad. Over the past three years, the annual cybersecurity spend as a percentage of revenue has grown consistently (figure 8).

In 2021, infrastructure security, the Internet of Things (IoT), industrial control systems (ICS), and operational technology (OT) together claimed roughly 20% of budget allocations, followed by threat intelligence, detection, and monitoring (14%) and cyber transformation (14%) (figure 9).

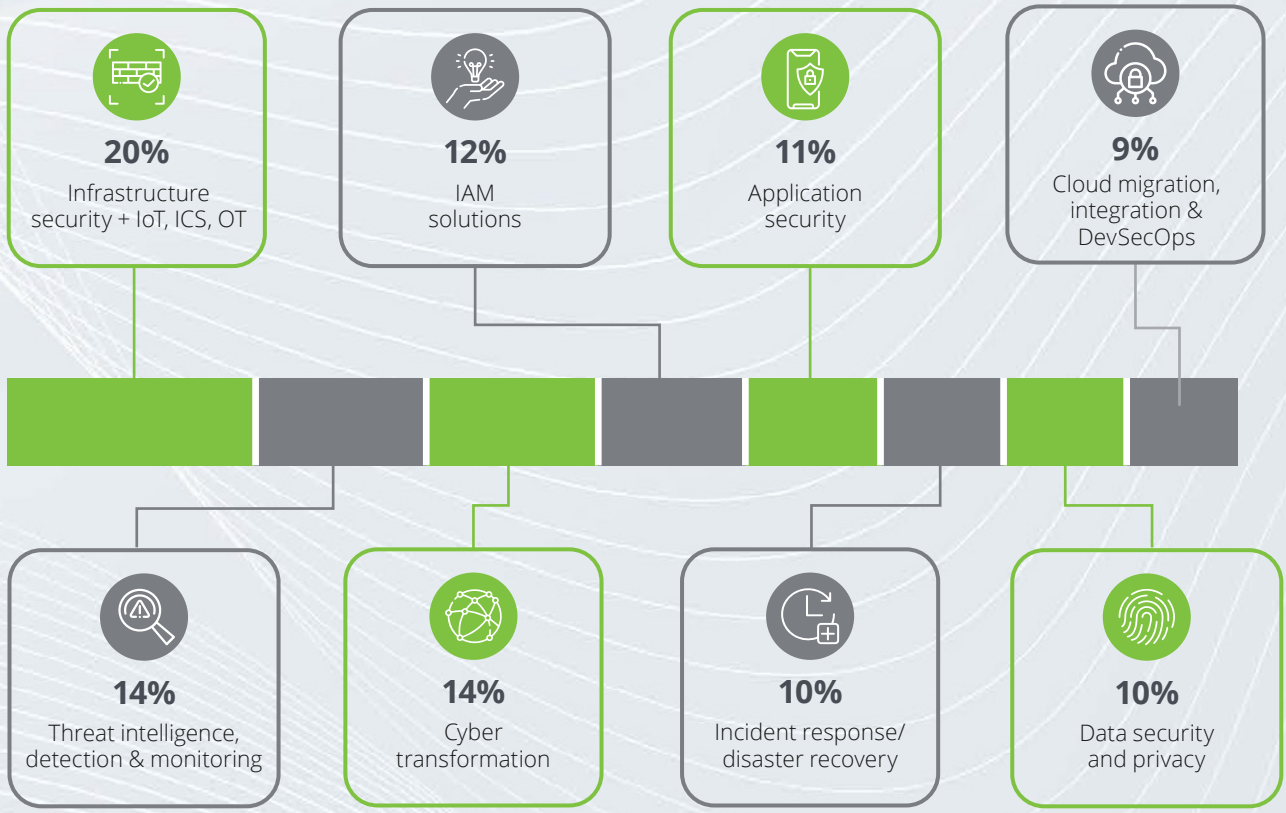
This compares to 2020 priorities, which saw 19% of budgets allocated to cyber monitoring and operations, 18% to endpoint and network security, and 16% to identity and access management.[14] To provide a measurable return on cybersecurity investments, CISOs may need additional tools in their risk management arsenals, including the adoption of risk quantification techniques.

Figure 8: Cybersecurity spend and revenue by sector



Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey"; Deloitte FS-ISAC Cyber Benchmarking Surveys, 2019, 2020

Figure 9: Budget allocation across cybersecurity domains



Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

Physician, heal thyself

Despite significant investment, human vulnerability remains #1. The top cyber threats cited by respondents are still phishing, malware, and ransomware and employee-related risks (figure 10).

Despite years of awareness of these trends, employees continue to fall prey to phishing, malware, and ransomware attacks, and persist in exposing their organizations to avoidable risk through both unintentional actions and deliberate malice.

While organizations are building resilience plans to counter these threats (figure 11), this approach focuses more on response and recovery than it does on true defense. Awareness training remains a priority, but is not sufficient on its own.

To further strengthen their defenses, 54% of surveyed cybersecurity professionals report that they are leveraging automated behavioral analytics tools to detect potential risk indicators among employees. That said, 25% continue to use leadership to monitor employee behaviors and risk indicators, and an additional 20% say they have no way to detect or mitigate these risks.

Figure 10: What is the top cyber threat your organization is most concerned about based on its business model?

Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

Figure 11: Which of the following actions have been implemented to increase your cyber and information security?

Source: Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."

Where to go from here

Cybersecurity practices in financial services continue to mature; executives and boards alike have prioritized cybersecurity spending and invested in emerging protocols to secure their extended enterprises against proliferating cyber threats. However, CISOs should continuously revisit their risk assessment approaches in line with continuously improving capabilities of cyber adversaries to stay 'on top of their game.' In our experience, CISOs have preferred maturity assessments to help prioritize spending but CEOs are increasingly calling for more sophisticated risk quantification techniques that tie into broader business risks.

The breathtaking pace of digitalization, remote work, and virtual customer engagement spurred by COVID-19 obliges CISOs to revisit many of their legacy cybersecurity practices. The persistent nature of certain threats—from phishing and malware, to extended enterprise control deficiencies and insider threats—simply underscores this imperative.

With remote work and digital transformation here to stay, it's time for financial services organizations to get more serious about embracing the cloud, securing the extended enterprise, focusing on a trusted customer experience , building resilient operations and remediating control gaps. This involves a multi-pronged approach that sees the adoption of more sophisticated incident detection and response capabilities, enhanced perimeter controls, improved risk identification methods, and more focused employee education initiatives. While there is no one-size-fits-all solution for stakeholders across the industry, it seems universally true that elevated risks will continue to compel new responses.

Endnotes

1. Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."
2. Ibid.
3. Ibid.
4. Ibid.
5. Identity Theft Resource Center, October 6, 2021. "Number of Data Breaches in 2021 Surpasses All of 2020."
6. Deloitte, July 24, 2020. "Reshaping the cybersecurity landscape."
7. Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."
8. Ibid.
9. Deloitte, October 21, 2019. "Executing the open banking strategy in the United States."
10. UpGuard, January 20, 2022. "The 6 Biggest Cyber Threats for Financial Services in 2022," by Edward Kost.
11. Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."
12. Ibid.
13. Ibid.
14. Deloitte, July 24, 2020. "Reshaping the cybersecurity landscape."

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.

Arjan Bajaj
Managing Director
Deloitte Risk & Financial Advisory
Cyber & Strategic Risk Services
Deloitte & Touche LLP
arbajaj@deloitte.com
+1 212 436 5277

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

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

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

Meghana Kanitkar
Senior Manager
Deloitte Risk & Financial Advisory
Cyber & Strategic Risk Services
Deloitte & Touche LLP
mkanitkar@deloitte.com
+1 212 436 5678

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

Deloitte.