The cyber clock is ticking: Derisking emerging technologies in financial services

McKinsey & Company

IIF Institute of International Finance

The Institute of International Finance
The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth.

McKinsey & Company
McKinsey & Company is a global management consulting firm deeply committed to helping institutions in the private, public, and social sectors achieve lasting success. For more than 90 years, our primary objective has been to serve as our clients' most trusted external adviser. With consultants in more than 100 cities and in over 60 markets across industries and functions, we bring unparalleled expertise to clients all over the world. We work closely with teams at all levels of an organization to shape winning strategies, mobilize for change, build capabilities, and drive successful execution.

As financial institutions actively adopt emerging technologies, they should act now to future-proof themselves against growing cyber risks.

About the authors

Lamont Atkins (lamont_atkins@mckinsey.com) is a senior adviser in McKinsey's Houston office, **Soumya Banerjee** (soumya_banerjee@mckinsey.com) is an associate partner in the New Jersey office, **Lauren Craig** (lauren_craig@mckinsey.com) and **Grace Hao** (grace_hao@mckinsey.com) are experts in the New York office, and **Justin Greis** (justin_greis@mckinsey.com) is a partner in the Chicago office. **Martin Boer** (mboer@iif.com) is a senior director for regulatory affairs for the Institute of International Finance (IIF) in Washington, DC, where **Melanie Idler** (midler@iif.com) is an associate policy adviser for IIF.

Contents

Executive summary

As financial-services companies around the world race to keep pace with a rapidly evolving technology landscape, they should consider not only what benefits new emerging technologies offer but also what risks they introduce.

To understand how companies are grappling with the best ways to use and protect the technologies of today and tomorrow, McKinsey partnered with the Institute of International Finance (IIF) to survey financial institutions around the world regarding their current and planned usage of ten key emerging technologies. (For details on research methodology, including the short-listing of top technology trends, based on global industry trends, see "Appendix: Approach and methodology.") How are companies approaching emerging technologies? What emerging technologies are they adopting? How do they plan to secure and mitigate the associated cyber risks? What cybersecurity capabilities will be needed to successfully adopt and secure new technologies?

Of the emerging technologies included in the survey (see sidebar "Ten emerging technologies"), a majority of financial-services companies indicated that they are prioritizing adoption of and investment in four of them: cloud and edge computing, applied AI, next-gen software development, and digital identity and trust architecture (Exhibit 1). All four technologies are likely to see quicker adoption than advanced connectivity, future mobility, immersive reality, quantum, machine learning, and Web3. This is perhaps because of their widespread applicability and maturity, as well as their proven, value-based use cases for financial-services companies.

While these technologies can provide exponential benefits, they can also bring cyber risks that companies must mitigate using their existing cybersecurity capabilities. The research shows that current capabilities are falling short of addressing these risks. Most survey respondents also recognize the need to strengthen critical cybersecurity capabilities, including third-party or supply chain management and privileged access management (PAM). As companies continue to increase their reliance on newer technologies, they must ensure they have thought through and implemented the necessary risk management capabilities. Otherwise, they may find the risks outweigh the benefits.

As the technology landscape in the financial-services industry continues to evolve rapidly over the next three to five years and as the associated risks mount, now is the time to future-proof the environment. Financial institutions can lay the foundations for action by asking themselves four questions about their pursuit of emerging technologies:

- Are we prioritizing the right technologies and cybersecurity capabilities? Are our technology priorities aligned with our security capabilities?
- Are we investing in the right technologies and cybersecurity capabilities?
- Do we have the right metrics and reporting? Can we, and do we, accurately and confidently measure against our risk appetite, provide transparency to regulators and executives, and identify strengths and weaknesses?
- Do we have the right talent to close capability gaps? Do we have sufficient and appropriate talent not just to maintain existing capabilities now but to support future maturity and technology expansions?

Ten emerging technologies

Cloud and edge computing. In cloud and edge computing, workloads are distributed across locations, such as hyperscale remote data centers, regional centers, and local nodes, to improve latency, data-transfer costs, adherence to data sovereignty regulations, autonomy over data, and security.

Applied AI (inclusive to generative AI). Models trained in machine learning can be used to solve classification, prediction, and control problems to automate activities, add or augment capabilities and offerings, and make better decisions. Note that at the time of the development and issuing of the survey, generative AI (the next generation of applied AI, which can automate, augment, and accelerate work by tapping into unstructured mixed-modality data sets to enable the creation of new content in various forms, such as text, video, code, and even protein sequence) was included as subset of the applied AI technology category.

Ten emerging technologies (continued)

Next-generation software development. New software tools, including those that enable modern code deployment pipelines and automated code generation, testing, refactoring, and translation, can improve application quality and development processes.

Trust architectures and digital identity. Digital-trust technologies enable organizations to build, scale, and maintain the trust of stakeholders in the use of their data and digital-enabled products and services.

Industrialized machine learning. A rapidly evolving ecosystem of software and hardware solutions is enabling practices that accelerate and derisk the development, deployment, and maintenance of machine learning solutions.

Web3. Web3 includes platforms and applications that aim to enable shifts toward a future, decentralized internet with open standards and protocols while protecting digital-ownership rights. It's not simply cryptocurrency investments, but rather a transformative way to design software for specific purposes. This shift potentially provides users with greater ownership of their data and catalyzes new business models.

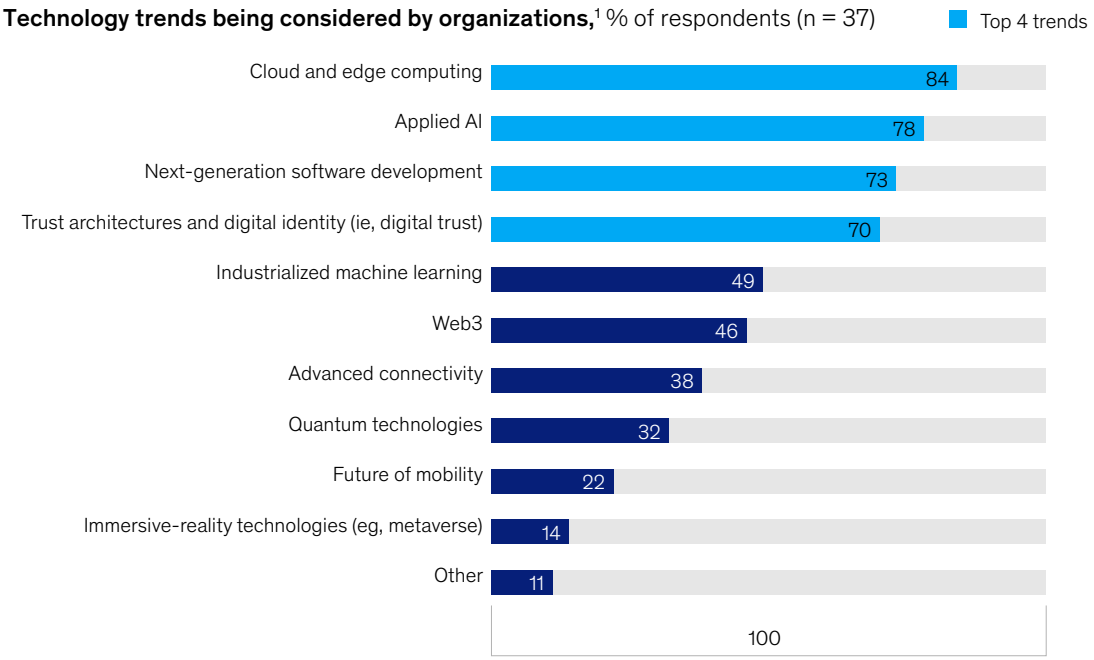
Advanced connectivity. Wireless low-power networks, 5G/6G cellular, Wi-Fi 6 and 7, low-Earth-orbit satellites, and other technologies support a host of digital solutions that can drive growth and productivity across industries today and tomorrow.

Quantum technologies. Quantum-based technologies could provide an exponential increase in computational performance for certain problems and transform communications networks by making them more secure.

Future of mobility. Mobility technologies aim to improve the efficiency and sustainability of land and air transportation of people and goods using autonomous, connected, electric, and shared solutions.

Immersive-reality technologies. Immersive-reality technologies use sensing technologies and spatial computing to help users "see the world differently" through mixed or augmented reality or "see a different world" through virtual reality.

Exhibit 1. **Among technology trends, cloud and edge computing are applicable to most financial-services organizations, followed by applied AI.**



[1]Question: Which technology trends are applicable (ie, have already been considered or discussed) to your organization?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Financial institutions have emerging technologies in their sights

WITH AN INCREASINGLY CROWDED AND FAST-MOVING TECHNOLOGY LANDSCAPE, COMPANIES ARE FACING PRESSURE TO KEEP UP.

Financial institutions must not only grapple with how to best employ and protect their current technologies but also pay more and more attention to the growing field of emerging technologies that promise to strengthen their businesses—offering benefits such as increased automation, scalability, and cost savings.

To better understand how institutions are approaching and prioritizing new technologies, we surveyed companies around the world about the applicability of ten emerging technologies to their businesses.

The survey results reveal that financial-services companies are not exploring all the emerging technologies equally. Instead, they are concentrating on those they perceive as most applicable to their organizations and likely to bring the most value, all while factoring in their current technological capabilities, their long-term business and tech strategies, and the potential regulatory impacts.

In recent years, financial-services companies have evolved into technology-driven companies. This tech-centric approach is visible in the ways they are prioritizing their investments; in addition to embracing software technologies, they are prioritizing investments in scaling technology development, such as DevOps (software development and IT operations), and industrializing machine learning and AI.

Institutions are also weighing the current level of maturity of each technology in their plans, considering the proven (and unproven) use cases that could add value to their businesses. The most applicable technologies were further along in their maturity journeys than some of those that were deemed less relevant.

Cloud and edge computing lead the list, with 84 percent of respondents recognizing their relevance to their businesses. Among those respondents, six in ten reported that more than 25 percent of their workload now resides in the cloud. This share will undoubtedly rise as cloud capabilities continue to evolve and as companies continue to transform their IT infrastructure through cloud migration and investment into cloud-native infrastructure—enticed by benefits such as flexibility, scalability, and cost efficiencies that are otherwise not offered by traditional, on-premise data centers.

Maturity and proven use cases undoubtedly help propel widespread adoption, and indeed survey respondents confirmed that cloud computing is already the most mature emerging technology used across financial-services companies. Over 70 percent of companies see their cloud adoption in the post-pilot stage, and 42 percent consider their capabilities fully adopted and in the maintenance stage.

Applied AI gets nearly as much attention, with almost 80 percent of respondents calling it relevant to their businesses. AI and machine learning have a long history in financial services. Corporate and investment banks, as well as insurers, were early adopters of AI and machine learning, decades before other financial institutions. The rest of the financial-services industry has caught up in recent years, and adoption has only continued to grow.

This aligns with broader technology trends in financial services, as applied AI technologies continue to evolve and offer the potential for increasing value to companies. The next stage of AI—generative AI—promises unprecedented disruption of the industry (see sidebar "The promises—and risks—of generative AI").

Unlike with cloud adoption, however, the maturity level of applied AI is still evolving. While many financial-services companies recognize the relevance of applied AI, most of their use cases remain in the early stages of development. Seventy percent of the survey respondents reported being in the pilot stage or earlier. Some use cases such as financial-crime, financial-risk, and asset modeling are quite mature. Those that are in the early stages include gen AI and large language models. Many institutions are still exploring their use in customer interaction support, personalized marketing, and fraud. These efforts offer companies the opportunity to gain a competitive advantage in the applied AI space before the technology is ready to be deployed. They can implement, for instance, proper oversight and responsible guardrails and controls for AI technology, thereby hastening its adoption for when it has sufficiently matured.

Almost 75 percent recognize the applicability of next-gen software development to their businesses, enticed by the ability to transform their software development life cycle and simplify previously complicated custom development tasks. AI-enabled development and testing, low-code and no-code tools, and other advances can improve processes and software quality in each stage of the development life cycle.

Next-gen software development is largely in the pilot stage across many companies. They stand to transform their software development life cycle, reaping the rewards of simplifying complicated tasks in custom application development. While only 11 percent of the survey respondents have fully adopted this technology, more than 50 percent are in the pilot or post-pilot expansion stage, indicating they have had time to consider the benefits and use cases of the technology.

Trust architecture and digital identity are also advanced across many companies. Almost

The promises—and risks—of generative AI

Generative AI (gen AI) has become a leader in emerging technology in 2024, creating widespread buzz across industry and media. In response, organizations are quickly finding ways for gen AI to propel sustainable, inclusive growth by solving problems efficiently. Our research estimates that gen AI could add $200 billion to $340 billion in value across banking, wholesale, and retail, and add $4.4 trillion in overall economic value.[1]

But gen AI introduces risks, including some we may not foresee today. Financial-services firms should prepare to recognize and mitigate those risks, applying the right resources, tools, and controls to protect their data, intellectual property, and reputation. Gen AI, for example, could certainly help banks, insurers, and money managers meet customers' needs, such as tailored advisory services, but raises new risks in terms of fairness and bias, as well as data ownership and governance.

[1] For more, see Michael Chui, Mena Issler, Roger Roberts, and Lareina Yee, *McKinsey Technology Trends Outlook 2023*, McKinsey, July 20, 2023; and *The economic potential of generative AI: The next productivity frontier*, McKinsey, June 14, 2023.

50 percent of the survey respondents put themselves in the post-pilot or maintenance stage of digital identity, and 70 percent call trust architecture applicable to their businesses, with use cases regarding digital banking, omnichannel customer experience, a 360-degree view of customers, and digital-wallet offerings. These efforts have demonstrated such benefits as faster innovation, stronger asset protection, and better customer experience, further persuading institutions to invest in underlying technologies, including zero-trust architecture, digital-identity systems, and privacy engineering.

Digital-trust efforts will most certainly increase as identity-related breaches, especially cyberattacks on identity systems, continue to grow. Eighty-four percent of companies participating in a 2022 Identity Defined Security Alliance survey reported suffering an identity-related breach during that year.[1] As organizations continue expanding their digital footprints, they must securely build and closely monitor their identity-related capabilities.

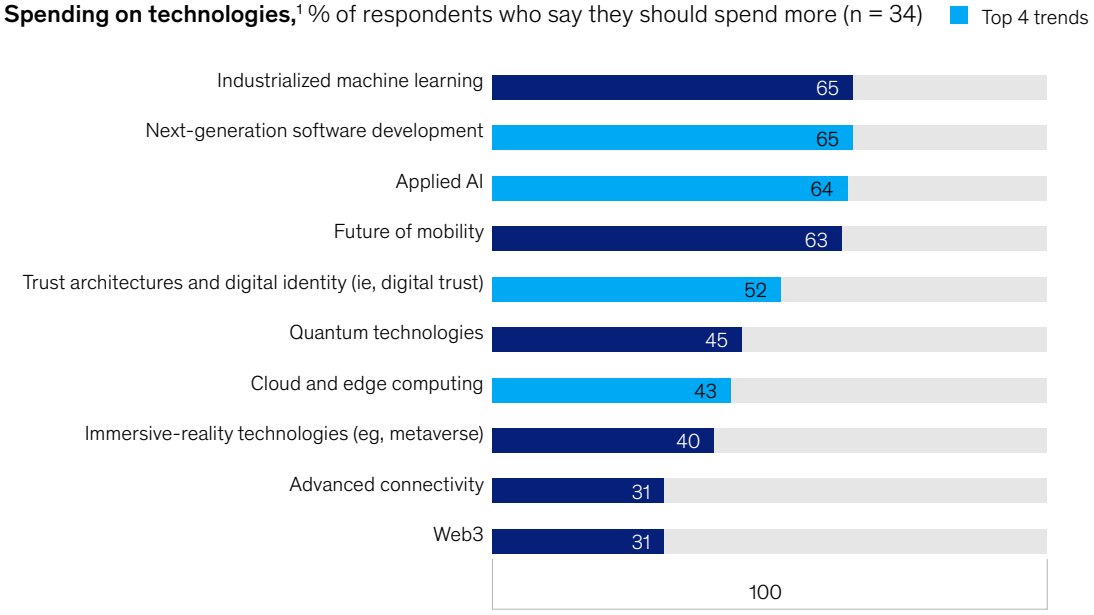
At the other end of the spectrum, less than one-third of the survey respondents are considering the following emerging technologies that stand to benefit financial-services companies applicable to their companies today: quantum, future of mobility, and immersive reality. Many institutions may not see adoption of these technologies happening soon and therefore are not prioritizing them today, because of the longer runway for adoption. It could well be that advances in quantum computing over the next few years may result in quantum quickly rising to a top concern, given its potential for materially affecting areas like password breaches and encryption breaking.

While this perspective is appropriate when considering the current maturity of these technologies, especially compared with more advanced and widely adopted technologies such as cloud and edge computing, financial-services companies should not be so quick to dismiss them. Quantum computing, for example, is estimated to bring over $600 billion in value to finance, with potential benefits such as real-time automated decision making and support activities such as holistic stimulations of liquidity or risk stimulations as part of large-scale, high-margin deals.

[1] "New study reveals 84% of organizations experienced an identity-related breach in the last year," Identity Defined Security Alliance press release, June 22, 2022.

Adoption and maturity of these technologies, and undoubtedly others, is only expected to expand, as companies believe they should be spending more on those perceived as most applicable to their organizations. Many noted that they do not believe they are spending enough on applicable technologies. More than half of the survey respondents recognize the need to spend more to continue building their capabilities in industrializing machine learning, next-gen software development, applied AI, future mobility, and trust architecture and digital identity (Exhibit 2). This spending imperative will only accelerate as the technologies ripe for investment continue to mature and proliferate.

Exhibit 2. Financial-services organizations are spending the most on cloud and edge computing technologies.



[1]Question: What percentage of the IT budget does your organization currently spend on tech trends?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Emerging technologies amplify existing risks and add new ones

EMERGING TECHNOLOGIES CAN OFFER SIGNIFICANT BENEFITS, BUT THEY CAN ALSO EXACERBATE EXISTING RISKS AND INTRODUCE NEW CYBER RISKS.

Cyber risk management is nothing new to financial-services companies, but the importance of a robust, comprehensive strategy has never been more critical and will only increase as institutions expand their technological footprint. Cyberattacks continue to increase, and financial-services companies face well-funded, highly organized, and well-trained cyber criminals. These criminals are also adopting emerging technologies to aid in their attacks, including recent attacks utilizing gen AI as part of sophisticated phishing campaigns.

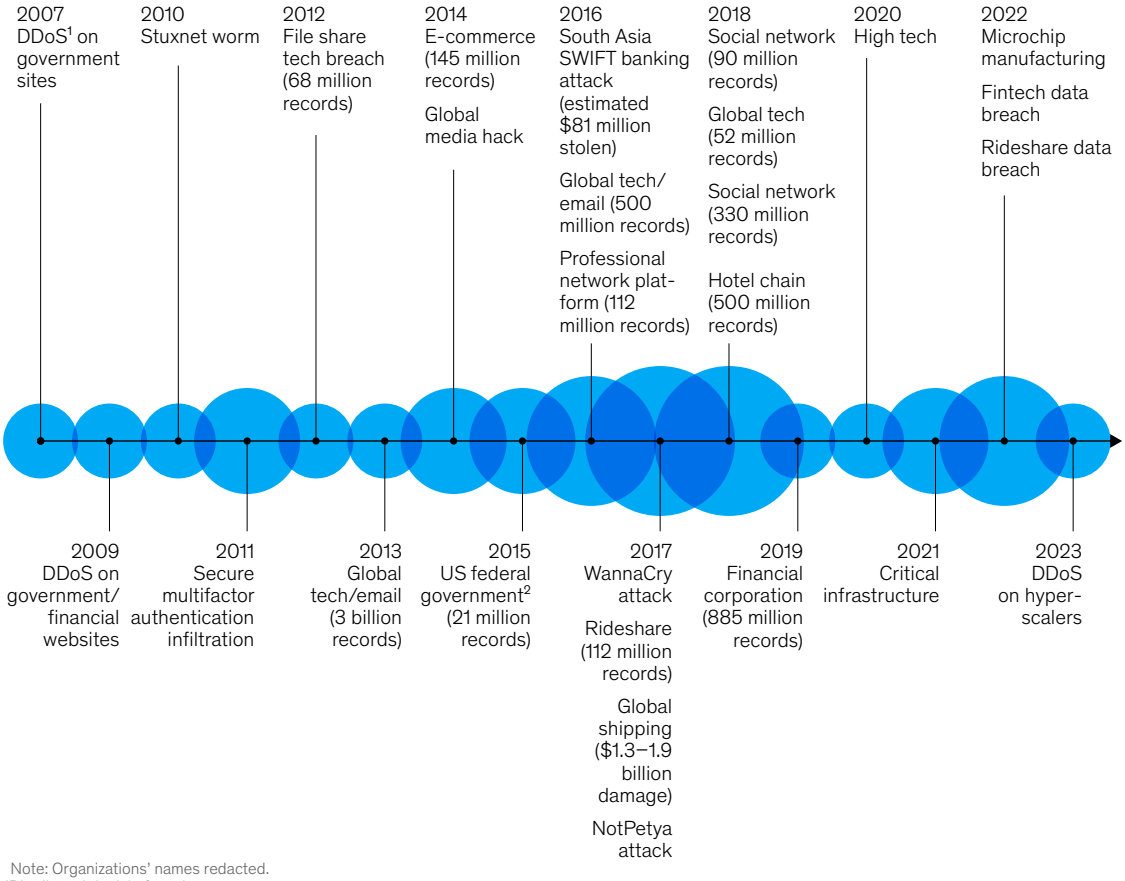
Cyber incidents are increasing in both frequency and severity year over year, and institutions must stay vigilant in their capabilities to defend themselves and protect their assets and finances against electronic crime (Exhibit 3). Cyber incidents are increasing in both frequency and severity year over year, and institutions should stay vigilant in their capabilities to defend themselves and protect their assets and finances. According to the 2024 CrowdStrike global threat report, Electronic Crime (eCrime) continues to rise and led as the most pervasive threat in 2023. Data-theft extortion also continues to rise, and 2023 saw a 76 percent increase in victims named on eCrime dedicated leak sites compared with 2022.[2] As companies increase their use of technology, they are also increasing the number of avenues for a potential cyberattack by mature threat actors.

We further surveyed financial institutions to better understand what cyber risks were top of mind. The biggest risks they reported that their organizations face include cyberattacks, AI, talent management, third-party and supply chain management, and data security (Exhibit 4). While this proves that companies are aware and considering the risks they face, it also raises a couple of questions: Do they

[2] *2024 global threat report*, CrowdStrike, February 2024.

Exhibit 3. **As financial-services organizations continue to transform and modernize, the frequency and severity of cyberattacks are increasing.**

Major cyberincidents, 2007–23



Note: Organizations' names redacted.
[1]Distributed denial of service.
[2]Sensitive personnel data stolen from US government employees who underwent security clearance background checks.
Source: Munich Re; McKinsey Global Institute analysis on the Future of Work after COVID-19

McKinsey & Company

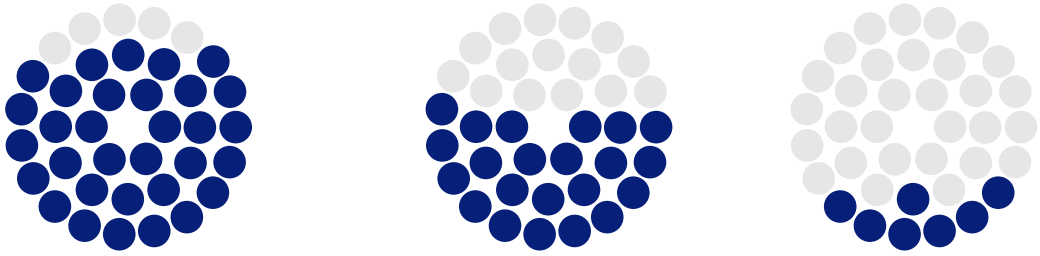
have the right capabilities to mitigate risks? Are they considering the potential for increased risks as they expand their adoption of new technologies? While they overwhelmingly recognize that they are under attack and that emerging technologies introduce risk, they still lack the appropriately skilled talent to address these risks.

As companies expand their technology adoption, cyber risks are likely to grow. Specifically, each of the four technologies that received the greatest attention from survey respondents introduces its own risks.

Take cloud migration, for example. As financial institutions move their workloads to the cloud and as network boundaries disappear, there's an increased risk of exposure to threat actors and of nation-states gaining access to networks. Without proper management anchored in a robust cloud security strategy and strong security capabilities, companies face a multitude of cyber risks, including misconfigurations, data privacy breaches, and data loss. Strong access controls, vulnerability management programs, data protection, and third-party management capabilities are critical to mitigating these risks; otherwise, organizations may find themselves susceptible to risks such as data loss through weak internal connections and service disruptions because of a heavy reliance on third-party exposure.

Exhibit 4. Cyberattacks, AI misuse, and talent management are key risks for financial-services organizations.

Top three cyber risks in next 3–5 years,[1] % of respondents (n = 37)



32 *of 37 respondents highlighted* ***cyber attacks*** *(eg, ransomware, fraud, social engineering, phishing, advanced persistent threat) as a top risk priority for their organizations. Attacks that exploit third parties and supply chains were singled out due to the difficulty in maintaining governance and visibility.*

22 *of 37 respondents highlighted* ***emerging technology and their potential misuse*** *(eg, AI risk, digital trust, cloud) as a key concern.*

7 *of 37 respondents highlighted* ***cyber talent management*** *as a concern, particularly with regard to upskilling, retention, hiring, and churn rate.*

[1]Question: What do you see as the top three cyber risks your organization will face over the next 3–5 years?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Applied AI and gen AI usage introduces significant regulatory risks for companies. Regulators are increasingly eyeing the risks associated with AI and are developing requirements, such as those set forth in the EU AI Act, that are likely to see enforcement in the coming years. Financial-services companies should build their security capabilities—including reporting, governance, and data privacy—in line with emerging regulations before they take force.

Next-gen software development and trust architecture can also subject companies to risks if they are not securely developed and implemented. Both technologies can provide increased efficiencies and increase security within an organization's technology environment, but with them comes the risk of failure in involving the right skills in development and implementation or of failure to integrate the technologies fully and securely into the environment.

Consider the implementation of zero-trust architecture. Security misconfiguration and integration issues associated with legacy tools may increase the risks of data loss, reputational harm, and insider threats.

Financial-services companies must rely upon their foundational cybersecurity capabilities to secure their technologies and protect their environments. Cybersecurity capabilities should be prioritized within the business as institutions continue to undergo technology transformations and recognize the benefits they bring with them. Without strong foundational security capabilities and controls within their cybersecurity programs, organizations will be exposed to risks brought on by their technology investments.

With this risk in mind, it is critical that organizations understand not only the benefits that new technologies may bring but also the accompanying risks. For institutions to truly harness their benefits, they must first coordinate their current capabilities by strategically investing in and maturing those that support the new technologies. While financial companies undoubtedly recognize the importance of cyber risks and the actions they should take to manage them, the question is, are they fully aware of the added risks these new technologies bring?

"Digital transformation is at the heart of our strategy. We recognize the importance of adopting and investing in emerging technologies, such as cloud and AI. At the same time, managing the associated cyber and technology risks is of utmost importance to ensure overall resilience of our vital services. This helps enhance the digital trust of our customers while protecting the safety and soundness of the bank."

—Jay Puthanveedu; global head of resilience, cyber and digital fraud; BNP Paribas

Companies need strong foundational cybersecurity capabilities to counter cyber risks

FINANCIAL INSTITUTIONS FEEL PRESSURE TO KEEP PACE WITH OTHER ORGANIZATIONS AND WORRY THEY ARE NOT INVESTING THE RIGHT LEVEL OF RESOURCES IN THE ADOPTION OF NEW TECHNOLOGIES.

Fifty-seven percent of surveyed respondents admitted they were concerned with keeping pace with emerging technologies, specifically with respect to their cybersecurity expenditures.

While they recognize the importance of having strong cybersecurity capabilities to mitigate cyber risks, 31 percent of companies are not confident that their capabilities can do so. To understand how companies are prioritizing and managing risks, we asked them to select their top strengths and weaknesses in their security capabilities across eight domains and numerous subdomains (Exhibit 5).[3]

The weakest capabilities they identified require immediate attention, as many of them are essential to successfully developing and deploying the five technologies of greatest interest to the survey respondents (Exhibit 6):

— *Third-party and supply chain management.* By far the greatest capability weakness—topping the list for 65 percent of survey respondents—third-party management is critical as companies continue to expand emerging-technology use in cloud computing and applied AI, which rely heavily on third-party services for such critical components as computing, data usage, model bias, model usage, and security.

As financial-services companies rely more and more on third-party services, they must enhance their own security capabilities to avoid exceeding their risk appetites and making their environments vulnerable to risks.

— *Metrics and reporting.* Despite compliance being an important factor for investment into cybersecurity, a significant portion of the survey respondents (41 percent) called their metrics and reporting capabilities a core weakness. Companies need reliable, insightful metrics

[3] Given the large number of sub-capability options, we focused our analysis on the top ten capabilities that received the largest number of respondent selections. We acknowledge that every cybersecurity organization is different, has varying remits and scope, and delivers different services depending on how the cybersecurity organization is defined for that company. While the capabilities and sub-capabilities in the model may change and evolve over time, we used this framework as a point-in-time standard to analyze the population of respondents in a consistent manner.

Exhibit 5. There are eight domains and numerous sub-domains in McKinsey's cybersecurity capability model.

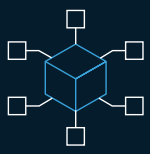
McKinsey cybersecurity capability model

Strategy, program management, and performance

- Security strategy
- Financial management
- Security vendor management
- Metrics and reporting
- Security project and program management
- Talent management
- Business relationship management
- Security service and product management
- Security team learning and development
- Communications management

Governance, risk, and compliance

- Security governance
- Third-party security risk management
- Digital transformation and integration
- M&A security
- Policies and standards
- Supply chain security
- Security assurance
- Cyber insurance
- Training, education, and awareness
- Security risk management
- Security compliance
- Insider threat program



Architecture and engineering

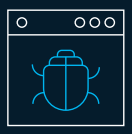
- Security architecture
- Operational technology security
- Secure software and product development
- Edge and IoT security
- Security engineering and integration
- Cloud security
- IT asset management
- Emerging technologies and innovation
- Security infrastructure and tooling
- Network and communication security
- Security consulting and advisory
- Threat modeling

Security operations and response

- Threat and vulnerability management
- Security incident response
- Security automation and orchestration
- Forensics and investigations
- Threat intelligence
- Application security testing
- Patch management and remediation
- Security logging and monitoring
- Endpoint security
- Threat hunting and active defense

Identity and access management

- Identity management
- Privileged access management
- Access management
- Cryptography and key management
- Identity and access governance
- Fraud protection



Cyber resilience and recovery

- Cyber crisis readiness
- Business continuity management
- Cyber crisis response
- Disaster recovery
- Cyber recovery and restoration

Data privacy and protection

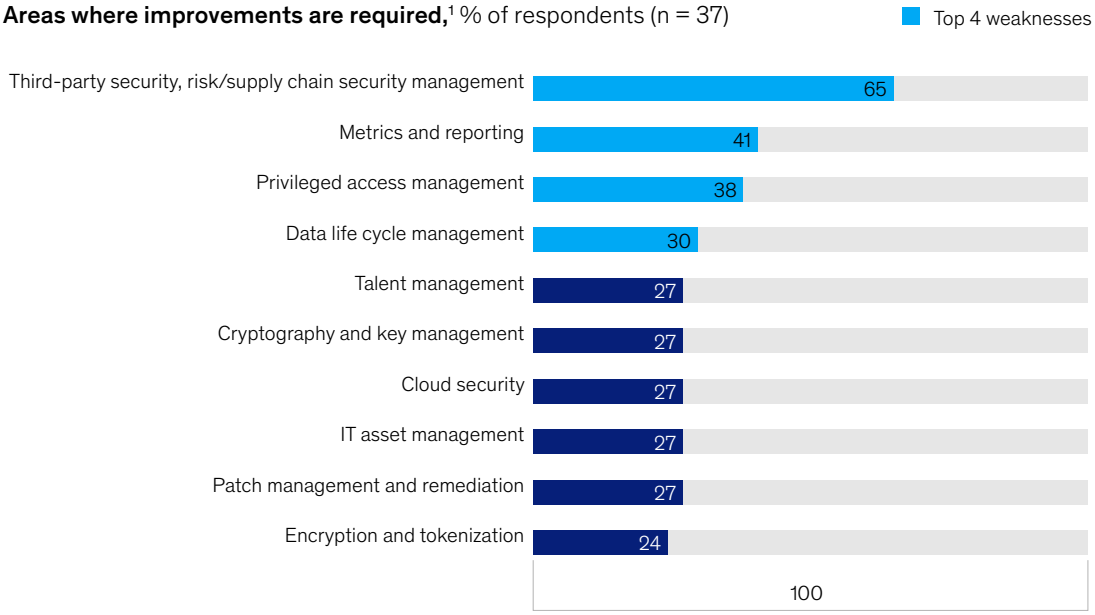
- Data loss protection
- Privacy operations
- Data life cycle management
- Encryption and tokenization
- Privacy compliance

Physical security and safety

- Facility security and physical access control
- Physical asset security
- Surveillance and monitoring
- Personnel and workforce security
- Executive protection

McKinsey & Company

Exhibit 6. **Financial-services organizations are often strong in overarching security governance and strategy but feel they could improve technical capabilities.**



[1]Question: My organization needs improvements in which areas (select up to 10 capabilities).
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

and reporting (such as security compliance, risk metrics, and vulnerability tracking) to prove to regulators the health of their security capabilities and to manage those capabilities. New regulations such as the US SEC Cyber Disclosure Rule[4] and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and similar regulations around the world have underscored the importance of better reporting, transparency, and governance of cybersecurity risk.[5] Additionally, with an increased focus around the world on regulatory compliance, operational resilience, as well as third-party risk management, more and more financial institutions are being challenged to prove the resilience of their vendors and their reliability in times of extreme stress. It is therefore more critical than ever that companies can measure their risks properly.

Without a robust process for measuring, reporting, and governing the risks associated with capabilities, organizations are flying blind, not knowing how much risk emerging technologies will pose. Companies, for example, will need evolved controls to measure model bias and risk, average time spent responding to incidents in the cloud environment, and the severity of vulnerabilities. These controls enable companies to identify their strengths and weaknesses and address those gaps before an issue materializes.

— *Identity and access management (IAM) capabilities.* The survey respondents passed similar judgment on their IAM capabilities, specifically the higher-risk PAM capability. Despite investment in digital identity and an increased technology domain to protect, companies are still struggling to protect

[4] US Securities and Exchange Commission, Release Nos. 33-11216; 34-97989: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, September 5, 2023.
[5] "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," Cybersecurity & Infrastructure Reporting Agency, accessed March 2024.

accounts with high-risk access. Without proper PAM, emerging-tech capabilities remain vulnerable to backdoor compromise by threat actors. In addition, as financial institutions increasingly depend on automated software development (like the next-gen software development that 74 percent of respondents are funding), they need to implement safe IAM and PAM practices.

— *The cloud.* The cloud expands the digital environment and overall attack vector that companies must secure. While they embrace digital trust, organizations struggle to manage digital identities. The automated deployment and easily scalable infrastructure in the cloud can increase the risk of data exposure. Unfortunately, developers often use domain administrator or master privileged accounts and default credentials in the cloud environment. Without proper PAM, they are practically inviting bad actors to grab the keys to the kingdom.

— *Data life cycle management.* While many financial-services companies are using next-gen software development and applied AI to pursue efficiencies and automation opportunities, they often fall short on the major foundational capability of data life cycle management, as 30 percent of the survey respondents admitted. Without secure, reliable data management in following best practices from creation to destruction, companies will have difficulty optimizing the benefits of technologies that require reliable data sources.

Think about applied AI. Securing the model training data to prevent tampering and the introduction of bias is essential. As AI models are applied to data sets and as data passes through the models, understanding the full life cycle of data security from discovery to classification, monitoring, compliance, and protection is equally essential. The top technologies in which institutions are investing also have the highest correlation with weaker capabilities. There is also a disconnect between the top-of-mind risks reported and the capability weaknesses companies are facing. These disconnects pose huge risks for organizations, especially as they continue to rapidly invest, pilot, and deploy these technologies in their environments. Organizations should strengthen these capabilities now to protect themselves in the future against the growing level of risk associated with these technologies.

How are companies prioritizing and investing in cybersecurity?

FINANCIAL-SERVICES ORGANIZATIONS' CYBERSECURITY CAPABILITIES ARE STRUGGLING TO KEEP UP WITH THE RAPID PACE OF ADOPTION.

To better understand how companies are approaching cybersecurity, we asked three important questions: What is causing organizations to mature their cybersecurity capabilities? How are they prioritizing spending on cybersecurity? Do they have the right talent to address their capabilities and gaps? (See sidebar "Cloud and edge computing—investments planned in tech but not security.")

Compliance advances cybersecurity maturity

As to what causes financial institutions to mature their cybersecurity capabilities, our survey found that there were two common factors across financial-services organizations: increased compliance with regulations and increased defense against outside threats. Seventy percent of companies said that increased compliance with regulations causes their organizations to mature their cybersecurity capabilities (Exhibit 7).

The desire for increased protection against security breaches comes as no surprise; it is the secondary top factor for maturity. Similarly, given increasing regulation of financial services, it is understandable that increased compliance with regulations would drive capability maturity, likely in areas with known gaps.

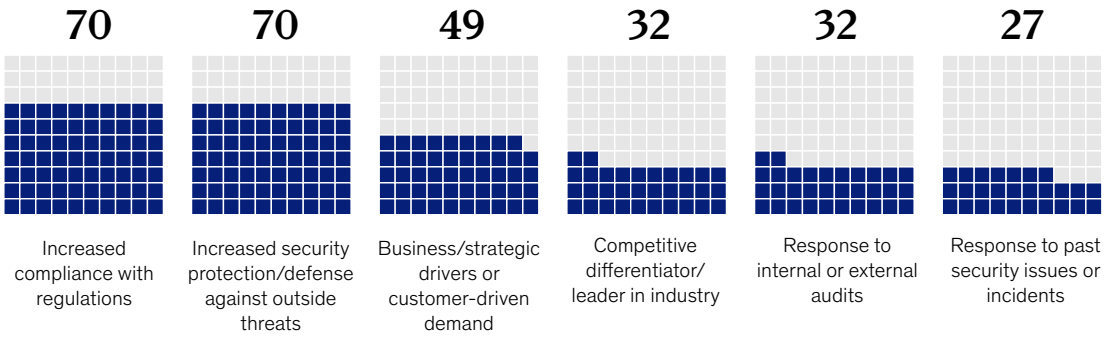
Companies should approach compliance as the minimum baseline of expectations rather than the aspirational goal. Likewise, regulatory compliance should be baked in proactively rather than a reaction or an afterthought, especially as rule makers delve into emerging technologies. For many technologies, regulations are still under development (most notably in the AI space). As regulations catch up with the level of adoption across organizations, companies need to be prepared to comply. By using compliance as an essential aspect of adoption, organizations can future-proof their technologies by getting ahead of emerging regulations before their implementation.

Spending habits: Companies recognize critical underinvestment in cybersecurity

Acknowledgment of underspending in capabilities has grown in the last three years. *Seventy percent of the survey respondents believe they are underspending and should spend more.* Not one organization reported overspending. This marks a shift from prior surveys: in the 2020 IIF and McKinsey Cyber Resilience Survey, only 58 percent of respondents acknowledged underspending. In 2023, a majority of companies

Exhibit 7. **Financial-services organizations value compliance and security against threats as top drivers for cybersecurity capabilities.**

Factors driving organizations in maturing cybersecurity,[1] % of respondents (n = 37)



[1]Question: What are the primary factors driving your organization in maturing its cybersecurity capabilities?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

said that they should increase cybersecurity spending more than 20 percent to build the requisite capabilities (Exhibit 8).

Today, financial-services companies devote 13 percent of their overall IT budget, on average, to cybersecurity. As they continue investing heavily in technologies, they should consider the short- and long-term implications of these technologies for cybersecurity to maintain protection of their environments.

Fortunately, cybersecurity spend is expected to increase over the next two to three years, with regional banks (Tier 2) expected to see the largest growth. Tier 2 banks' anticipated cybersecurity spend likely comes as they near the Tier 1 capital threshold and anticipate increased scrutiny from regulators (Exhibit 9).

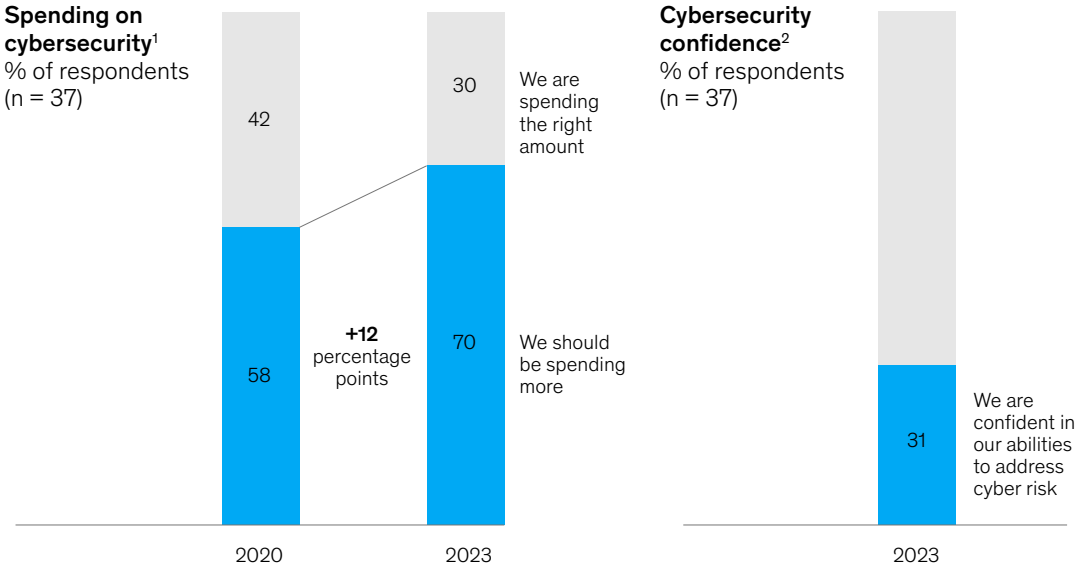
A portion of the expected increased funding is likely to go toward special initiatives to address growing cyber risk. Many companies also acknowledge that they are not currently prepared to mitigate risks associated with emerging technologies and that they must implement special initiatives and controls to secure their environments. But with the ever-increasing need for additional funding, special initiatives will only add to existing budget strains.

More than 40 percent of the survey respondents have launched special initiatives to address the security control gaps related to the adoption of emerging technologies (Exhibit 10). Fewer than 10 percent lack plans to invest in protecting the top four technologies.

"A key to enhanced security for emerging and critical technologies is to develop standards on how current cybersecurity and information security measures are integrated into the use of these technologies. Tighter integration between these standards and current cyber frameworks, such as ISO and the National Institute of Standards and Technology's CSF, will create uniformity in how these technologies are implemented between financial institutions and the agreed security measures for these technology usages."

—Jason Harrell; head of external engagements, operational and technology risk, Depository Trust and Clearing Corporation

Exhibit 8. **The lack of investment in capabilities has grown in the last three years as financial firms continue to acknowledge underspending in cybersecurity.**



[1]Question: I believe we should be spending (more/less/the same) on our cybersecurity program.
[2]Question: Do you currently feel you have the appropriate level of full-time cybersecurity employees?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Cloud and edge computing—investments planned in tech but not security

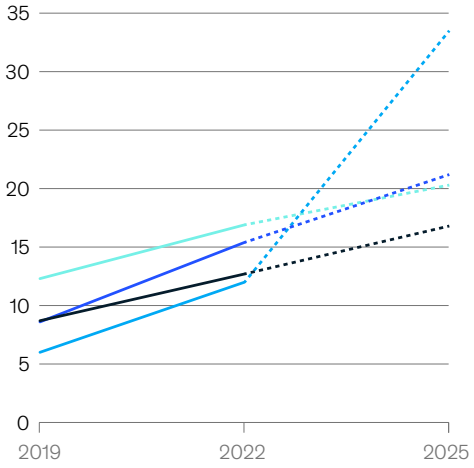
While more and more financial institutions are moving to the cloud, not enough are paying sufficient attention to the security risks associated with the cloud environment. Although 84 percent of the survey respondents consider cloud and edge computing applicable to their businesses and about 70 percent have entered the post-pilot phase of cloud implementation (reflecting heavy reliance on cloud technology), few are planning to invest in robust cloud security. Almost 30 percent plan to maintain or reduce costs, even as they invest more in cloud technology.

This may stem from the belief that cloud service providers will manage all security capabilities for firms. While they certainly manage some security, it is not a one-sided equation; organizations must prioritize protecting themselves and implement secure controls and practices for the security of their cloud environments under their purview.

Third-party security risk and supply chain security management was the number-one cybersecurity capability weakness reported by survey respondents. Given that cloud computing and cloud security rely heavily on third parties, firms should think twice about reducing their investment in cloud security and continue to upskill their talent to ensure they are building secure practices "by design" into their cloud environments.

Exhibit 9. In the US, Tier 2 regional banks are increasing their spend on cybersecurity relative to IT.

Planned cybersecurity spend as a share of IT budget, by type of bank,[1] % (n = 26)



		Assets under management	Number in 2022
Mega	Tier 0	>$1 trillion	4
	Tier 1	>$0.1 trillion–$1.0 trillion	30
Super regional	Tier 2	>$50 billion–$100 billion	16
Regional	Tier 3	>$5 billion–$50 billion	223
Midcap and credit unions	Tier 4	>$1 billion–$5 billion	707
	Tier 5	>$0.5 billion–$1.0 billion	771
	Tier 6	≤$0.5 billion	2,952
	Credit unions	–	4,866

[1]Banks assigned to capital tiers using self-reported revenue ranges, based on an assumed profit margin of ~15% and presumed return on assets of 1.18%.
Source: SNL Financial; McKinsey Cyber Market Map

McKinsey & Company

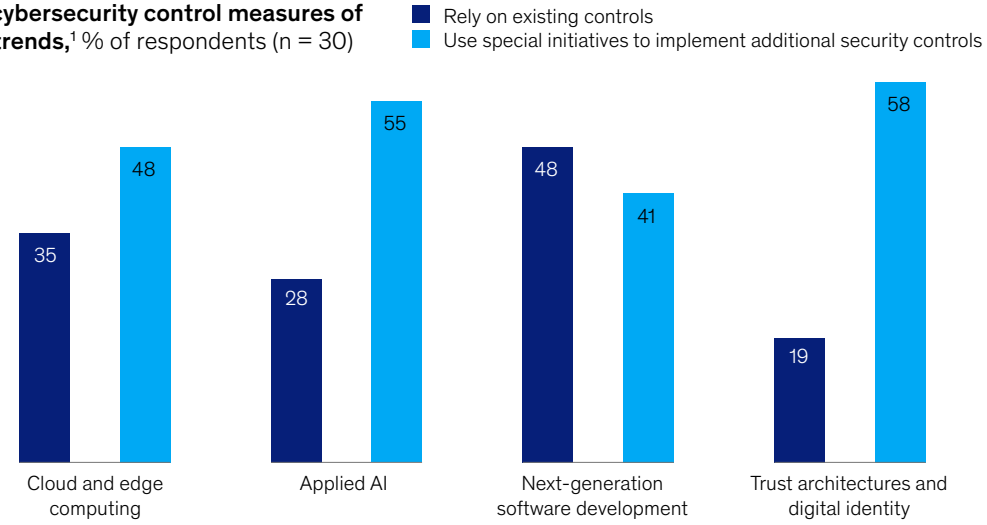
Companies rely on talent to address capability gaps

Efforts to close security capability gaps typically revolve around recruiting new talent and upskilling existing talent. All respondents reported relying on existing talent, as well as new talent, to secure their technologies. However, 65 percent noted concerns about gaining and retaining appropriately skilled cybersecurity talent. While companies can outsource some cybersecurity work, more than half of the respondents plan to rely on internal resources to close the capability gaps related to their emerging technologies (Exhibit 11).

Financial-services companies may encounter obstacles in finding and retaining the right talent to handle their particular security risks, as talent attraction and retention is an ever-growing concern for cybersecurity more broadly. They should consider other options, including the use of technology to augment talent—making gen AI a copilot in security operations, for example.

Exhibit 10. More than 40 percent of respondents are utilizing special initiatives to secure each of the top four tech trends.

Planned cybersecurity control measures of top tech trends,[1] % of respondents (n = 30)

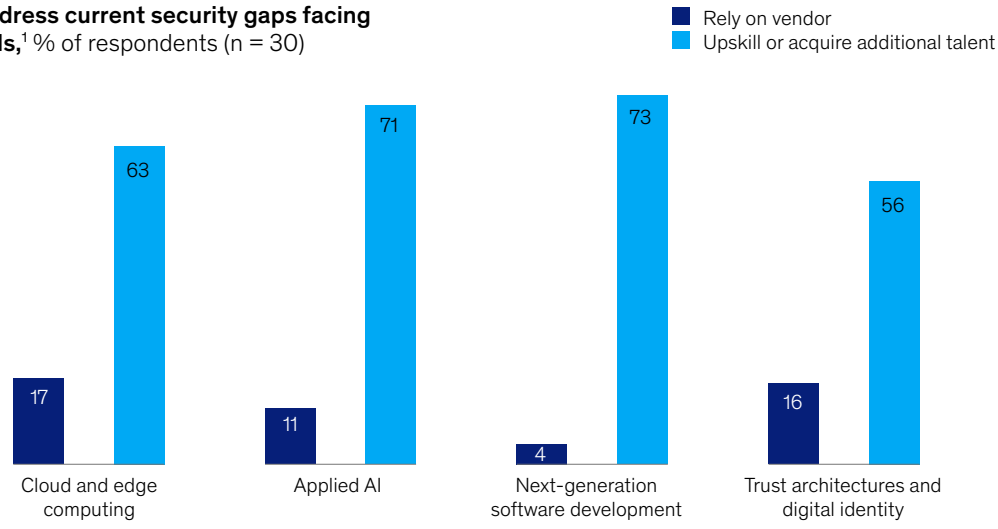


[1]Question: Describe the cybersecurity control measures you are planning on implementing to secure the top tech trends.
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Exhibit 11. More than 50 percent of respondents are planning to address security gaps for each of the top four tech trends with internal resources.

Plan to address current security gaps facing tech trends,[1] % of respondents (n = 30)



[1]Question: How are you planning on addressing the current security gaps your organization is facing on the top tech trends?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Call to action: Future-proof the environment

THE TECHNOLOGY LANDSCAPE IN THE FINANCIAL-SERVICES INDUSTRY WILL EVOLVE RAPIDLY OVER THE NEXT THREE TO FIVE YEARS, ACCOMPANIED BY MOUNTING RISKS.

Technologies that are popular today may change tomorrow, and as use cases develop and mature, companies are likely to continually reassess their applicability and investment priorities. The time for action to future-proof the environment is now. Our survey found that even leading institutions are falling short and that smaller companies with significantly less budget or ability to attract top security talent face even greater challenges.

Financial institutions should lay the foundation for action by asking themselves the following four questions about their pursuit of emerging technologies:

— *Do we have the right technology priorities, and are they aligned with our security capabilities?* Expansion into newer technologies, such as the cloud and applied AI, usually means greater reliance on third-party services. Companies should reflect on their capabilities and the maturity of their security before introducing any technology. The third-party risk management capability warrants special attention.

— *Do we have the right metrics and reporting?* Whether to satisfy regulators or to hold teams accountable, financial-services companies need transparent, value-based metrics for managing cyber risks. They can aid in monitoring performance, informing decisions, and identifying emerging issues for quick action. These metrics should measure cyber risk from an emerging-technology perspective and be reported appropriately to the right stakeholders, including board members and executives, lines of defense, and the risk management team.

— *Are we investing in the right things?* Decisions on technology investments should take security capabilities, especially IAM capabilities, into account. The growing risk of security breaches and the looming need for regulatory compliance shine a spotlight on these capabilities.

— *Do we have the right talent and technology to close capability gaps?* Every organization needs to invest in talent, but hiring and retaining the right talent is a challenge and calls for exploring other ways to fill the talent gap, such as utilizing emerging technologies themselves, including AI.

Emerging technologies are grabbing lots of attention in the financial-services industry. Each brings cyber opportunities and risks. Most companies will have to build their cybersecurity capabilities to handle the risks. Today is the time to future-proof the environment, ensuring success for tomorrow.

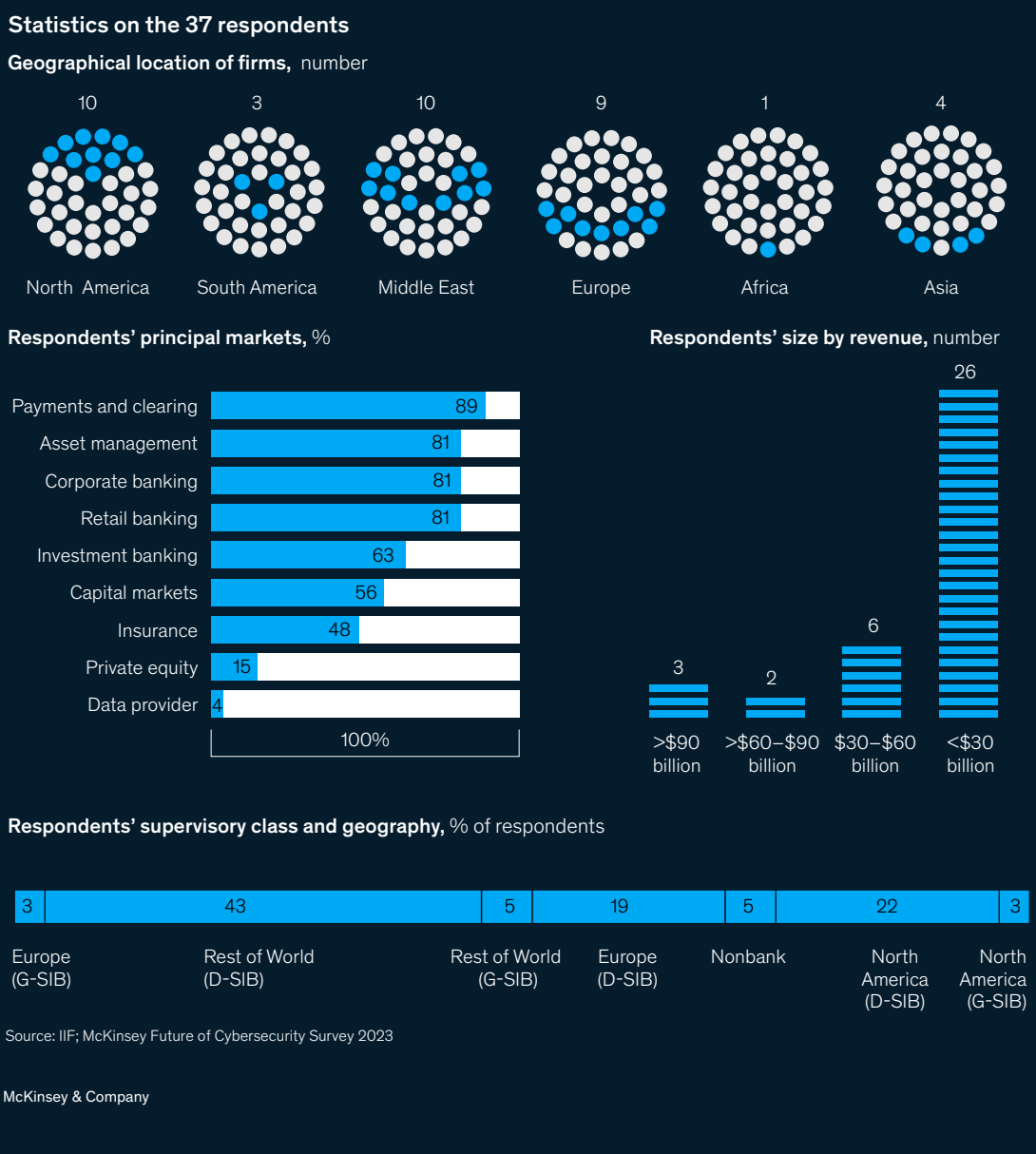
Appendix: Approach and methodology

The insights in this report were derived from a 2023 survey of 37 financial-services companies around the world.

The institutions surveyed included asset managers and private equity companies; retail, corporate, and investment banks; payment companies and clearing houses; capital markets; insurers; and a major data provider. Twenty-six of the institutions reported less than $30 billion in annual revenues, and five reported at least $60 billion (exhibit).

To help structure and streamline our survey, we referred to the National Institute of Standards and Technology's Cybersecurity Framework, industry technology trends, and previous McKinsey and Institute of International Finance (IIF) survey questions.

Exhibit. **A total of 37 financial-services firms participated in the survey, broken down by principal market, revenue, and supervisory class and geography.**



Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

McKinsey & Company

March 2024