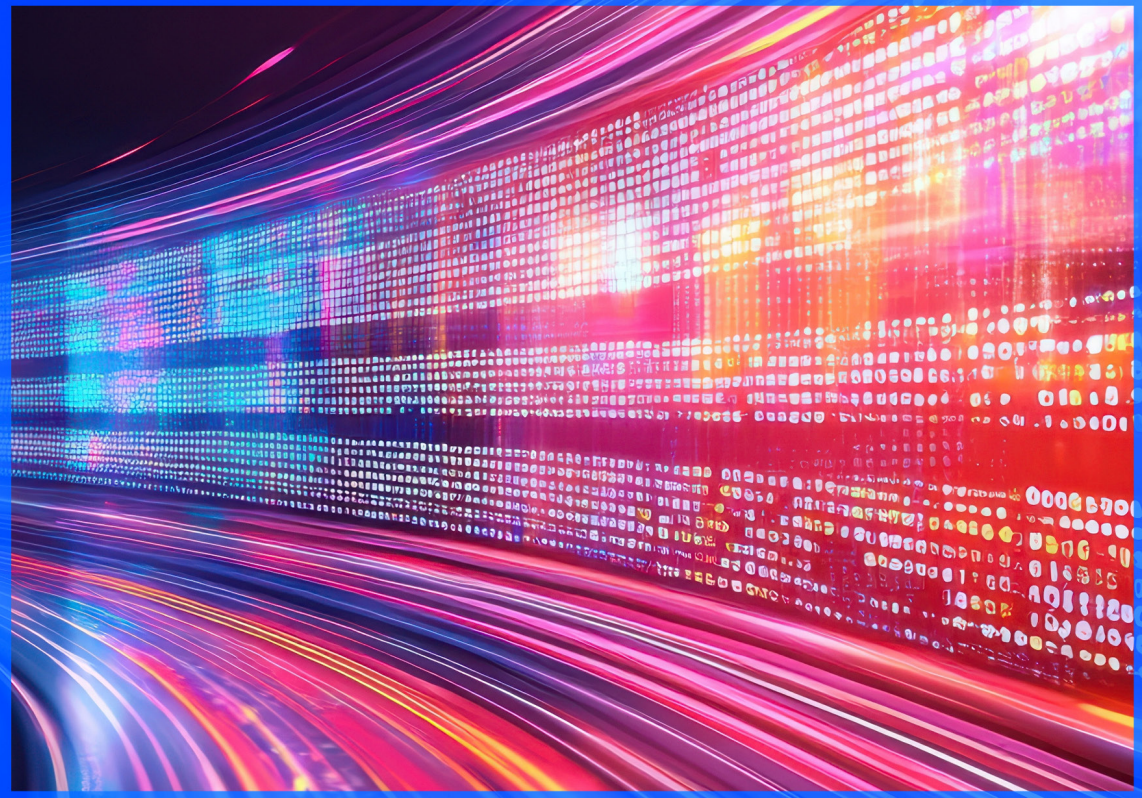
Cyber and Technology Risk Survey 2026

Financial Services (FS)



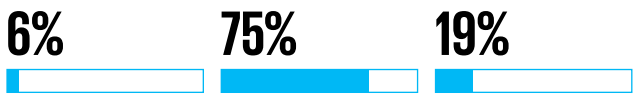
The 2026 KPMG Cyber and Technology Risk Survey captured perspectives from 310 senior leaders across the United States, including 72 from the financial services (FS) sector. The results provide a comprehensive view of the FS cyber risk landscape, where recurring cyber breaches—particularly denial-of-service and phishing attacks—are driving business disruption across operations, supply chains, and customer trust.

Cyber disruption is no longer episodic for financial services—it is systemic

Cyber disruption in financial services is no longer an isolated or episodic risk—it is persistent, frequent, and deeply embedded in day-to-day operations. Most organizations report multiple cyber breaches in the past year, with denial-of-service and phishing attacks occurring at higher rates than in other sectors. These attacks are directly disrupting supply chains, communications, and operational continuity. Cascading business impacts include erosion of customer trust, reduced productivity, and heightened operational strain—signaling a sector-wide shift from managing individual incidents to sustaining resilience under constant pressure.

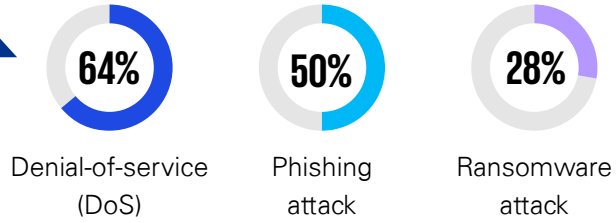
Increasing cybersecurity threats[a]

Cyber breach incidents in past 12 months



Top three security breaches among FS organizations (N=58)[b]

Highest in FS sector compared to other sectors



Top three impact areas of cyberattacks on FS organizations

50%
Supply chain and communication disruptions

47%
Loss of customer trust and decreased brand value

44%
Reduced productivity and efficiency across operations

As cyber risk escalates, financial services organizations are facing significant business disruption, including supply chain impacts, erosion of trust, and reduced productivity and operational efficiency.

"Supply chain and communication disruption" emerges as the most significant impact of cyberattacks for FS organizations, the highest across all sectors

Note(s): (a) Sum of percentages may not add up to 100 due to rounding; (b) N value is different for this theme as it is based on a logic-driven question

Source(s): Cyber and Technology Risk Survey, 2026

AI is deemed essential, but its adoption is slow in FS cybersecurity operations

Among financial services organizations, AI adoption across cybersecurity functions remains uneven and limited. Most organizations are still in the experimental or partial-implementation stages, with only a small share having fully integrated AI across security operations. AI utilization is concentrated in high-impact control areas such as identity and access management, malware defense, and threat intelligence, where automation delivers immediate benefits. However, operational complexity, lack of trust in AI decision-making, and challenges demonstrating value at scale continue to slow broader deployment.

Maturity level of AI integration[a]

AI integration and deployment across cybersecurity function

1% No AI capabilities have been implemented

60% Partially implemented in specific areas

28% Experimental/pilot phase

11% Fully integrated across the organization

AI utilization in cybersecurity areas

Top three cybersecurity areas with high AI utilization (N=71)[b]

Malware detection and prevention

Identity and access management

Threat intelligence and detection

Challenges of using AI in cybersecurity[c][d]

Rank 1 Massive effort required to set up and train AI solutions

Rank 2 Trusting that AI recommendations are accurate, reliable, and explainable

Rank 3 Lack of internal knowledge and difficulty in demonstrating ROI of AI solutions

Based on weighted average score(c)

Expected benefits from AI-driven automation in cybersecurity

Top three benefits from AI automation (N=71)[b]

AI-driven automation is expected to enhance cybersecurity outcomes in FS by improving operational visibility, freeing up resources, and supporting talent retention.

37% Better measurement and reporting on security operations

34% Increasing productivity; freeing up resources

34% Attracting and retaining top security talent

Note(s): (a) Sum of percentages may not add up to 100 due to rounding; (b) N value is different for this theme as it is based on a logic-driven question; (c) Weighted average of the ranks has been calculated by assigning 50% weight to Rank 1, 30% to Rank 2, 20% to Rank 3; (d) Top ranks have been highlighted based on figures rounded to two decimal points, with data having higher decimal precision within the same percentage considered higher

Source(s): Cyber and Technology Risk Survey, 2026

Operational complexity—not lack of awareness—remains the biggest barrier to cyber resilience

Operational complexity has emerged as the dominant challenge to effective cyber risk management in financial services. Fragmented security systems, legacy infrastructure, and limited visibility into networks and endpoints are slowing both threat detection and remediation. Compounding these challenges are workforce constraints, integration issues, and insider risks, increasing exposure. At the same time, attackers are leveraging AI to scale malware, automate social engineering, and exploit supply-chain vulnerabilities, further amplifying risk. As both internal and AI-driven threats accelerate, the sector faces mounting pressure to simplify environments, strengthen integration, and close execution gaps across the security lifecycle.

Barriers to threat management

Top three barriers to threat identification

56%
Complexity of IT infrastructure

50%
Fragmented security systems and lack of integration

38%
Limited visibility into network and endpoints

Top three barriers to threat remediation

51%
Technical complexity and legacy systems

46%
Vendor patching delays and inadequate support

44%
Inadequate vulnerability prioritization and risk assessment

Source(s): Cyber and Technology Risk Survey, 2026

Top three high-impact cybersecurity challenges

53%
Lack of qualified professionals

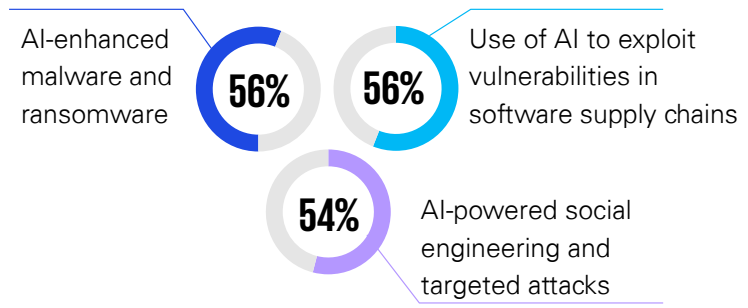
51%
Insider threats and employee awareness gaps

49%
Technological integration issues and geopolitical risks

Cyber resilience in financial services is increasingly shaped by people and integration challenges, as talent shortages, insider risk, and complex operating environments elevate overall exposure.

AI-driven and internal threats

Top three AI-driven threats



Top three internal threats

61% Malicious use of AI tools by insiders (e.g., data exfiltration)

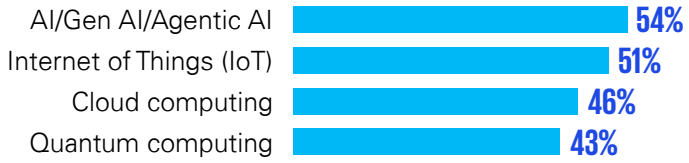
54% Accidental data breaches facilitated by AI tools (e.g., misconfigurations)

46% Use of generative AI to create malicious code/bypass security

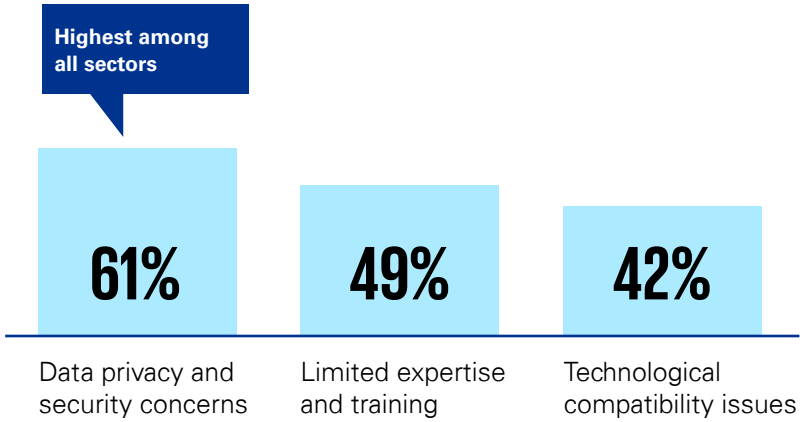
Emerging technologies are accelerating risk faster than governance can keep up

Rapid adoption of emerging technologies is expanding the cyber risk surface faster than governance and controls can keep up. Financial services organizations identify AI, cloud, IoT, and quantum computing as high-impact threats, yet readiness levels vary widely. Quantum risk, in particular, highlights the disconnect between awareness and preparedness—while widely recognized as a future threat, mitigation efforts remain largely exploratory. Responsible AI adoption is similarly constrained by persistent data privacy concerns, skills gaps, and technology compatibility challenges. Post-quantum cryptography is gaining traction through pilots and early implementations, but overall readiness underscores the need for more coordinated, forward-looking risk management.

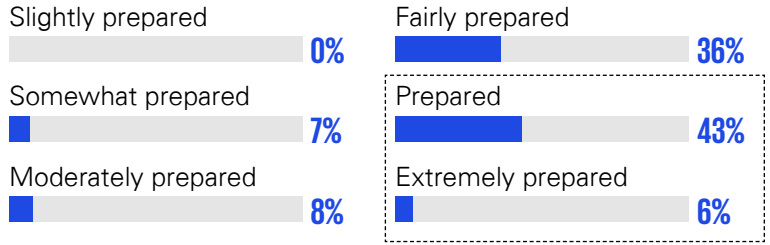
Top high-impact emerging-technology threats



Top three obstacles to enabling responsible use of AI

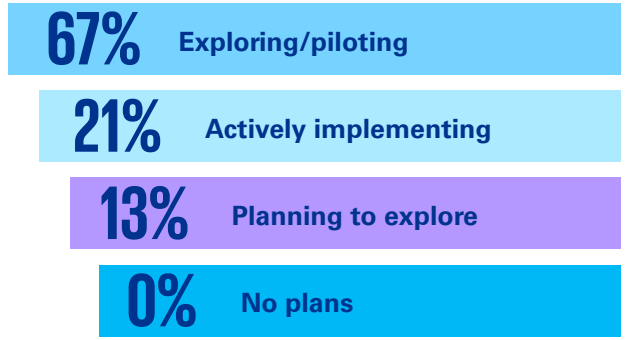


Preparedness to mitigate quantum computing risks[a]



Almost half of FS organizations believe that they are well prepared to address quantum computing threats

Post-quantum cryptography adoption status[a]



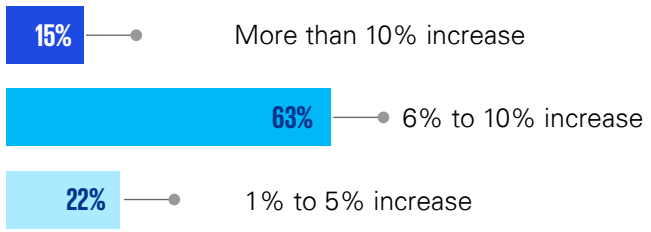
Note(s): (a) Sum of percentages may not add up to 100 due to rounding. | Source(s): Cyber and Technology Risk Survey, 2026

Investment is increasingly focused on foundational security and AI enablement

Cybersecurity investment in financial services is expected to increase over the next two to three years, reflecting sustained prioritization of resilience amid an increasingly complex threat environment. Spending is heavily focused on foundational capabilities such as data security, cloud security, and vulnerability management, while a growing share of budgets is being allocated to AI-related cybersecurity initiatives. However, securing funding remains challenging, with leaders citing difficulty demonstrating ROI, navigating technical complexity, and limited resources for developing investment cases. As budgets grow, organizations are aligning investment decisions toward measurable impact—balancing innovation with the need to strengthen core defenses.

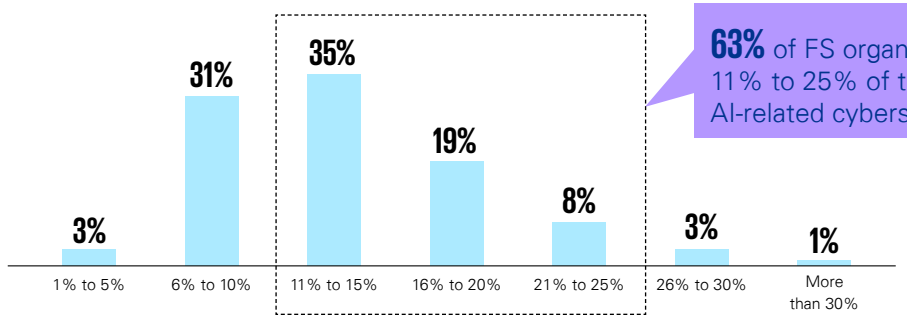
Budget allocation for cybersecurity

Anticipated budget change over the next 2–3 years



Budget dedicated for AI[(a)]

Percentage of budget allocated to AI-related cybersecurity initiatives



Priorities for cybersecurity investments[(b)(c)]

	Current	Next 2–3 years
Rank 1	Cloud security	Data security and privacy
Rank 2	Data security and privacy	Cloud security
Rank 3	Vulnerability management and remediation	Threat intelligence and detection
	Based on weighted average score(b)	Based on weighted average score(b)

Top three challenges to securing cyber budget increases

Difficulty demonstrating ROI of cybersecurity investments

Complexity of the cybersecurity landscape

Limited resources for developing budget proposals

Note(s): (a) Sum of percentages may not add up to 100 due to rounding; (b) Data represents weighted average of the ranks that has been calculated by assigning 50% weight to Rank 1, 30% to Rank 2, 20% to Rank 3; (c) Top ranks have been highlighted based on figures rounded to two decimal points, with data having higher decimal precision within the same percentage considered higher

Source(s): Cyber and Technology Risk Survey, 2026

What's next for the financial services CISO?

The findings in this report make one thing clear: The old paradigms of cybersecurity are no longer sufficient for the financial services industry. The modern CISO is tasked with defending an expanding and evolving digital frontier. The journey from a reactive to a predictive security posture is challenging but essential. Simply bolting on another tool only adds to the cacophony of siloed and legacy systems and fails to address the challenges of architectural complexity, the explosion of NHIs, and the dual-use nature of AI. These along with operational complexities, persistent talent gaps, and budgetary pressures create unique challenges for CISOs across financial services sectors. These are not individual problems to be solved. Rather, they are interconnected forces that are fundamentally reshaping the risk landscape.

Why does this matter? Because in an era where cybersecurity is a top concern for chief executives, the CISO is at a critical fork in the road. The choice is between two distinct paths: one that leads back to a reactive posture, buried in the fog of endless security alerts, and another that leads forward in a direction defined by a unified data architecture, a strategy for building trust in AI, and the ability to translate the language of vulnerabilities into the language of business value.

This is the difference between being a cost center and being a strategic partner. The ultimate takeaway is that the CISO must evolve from being a defender of technology into a protector of business value.

The following action steps are not just a security checklist; they are also a guide to embedding this mission into the heart of your organization.

Establish a formal AI security and governance program. Champion AI as a force multiplier for your team, not as a silver bullet. Build trust and ensure operational safety by implementing a robust framework for testing models and ensuring a "human in the loop" for all critical decisions.

Focus on foundational "blocking and tackling." While emerging threats are important, mastering the fundamentals of security operations, data security and privacy and identity governance provide the strongest defense against most cyberattacks.

Implement counter measures for emerging threats. AI based attacks including novel day zero exploits and deepfakes present challenges to legacy controls. Implement preventative and detective technologies to defend against the proliferation of autonomous attacks.

Build a unified security data architecture to combat complexity. Break down the silos among your security tools. A unified data lake is the foundation for achieving the analytical speed and clarity needed to stay ahead of adversaries in the AI offense/defense arms race.

Govern all identities, human, and nonhuman. The exponential growth of machine and agentic identities requires a new governance model. CISOs are encouraged to work with the business to establish controlled processes for provisioning and monitoring these identities to close a rapidly expanding security gap.

Start planning for a post-quantum world. Most financial services organizations (88%) are already exploring, piloting, or implementing post-quantum cryptography. Accelerate your journey of quantum readiness by creating an inventory of your cryptographic systems, upskilling talent, and developing a multi-year roadmap for migration. Educate your board on the "harvest now, decrypt later" threat to secure the necessary long-term investment.

Vet your partners for deep technical expertise. As you increasingly rely on MSPs and consulting firms, prioritize partners based on their expertise and their AI/automation capabilities. Ask the hard questions to determine if a partner can truly help you achieve your goals for speed and safety.

> The greatest vulnerability in financial services today isn't a sophisticated zero-day exploit; it's our own operational complexity. We are drowning in siloed tools and fragmented data while adversaries move laterally in milliseconds. The CISOs who lead the next decade will be the ones aggressively dismantling complexity to build unified, predictive architectures and engineer deep business resilience."
>
> —Matthew P. Miller, Global Financial Services Cyber and Technology Risk Lead, KPMG LLP

Contact us

Matthew P. Miller
Global Financial Services Cyber and Technology Risk Lead
KPMG LLP
E: matthewpmiller@kpmg.com

Manish D. Madhavani
US Financial Services Leader
KPMG LLP
E: mmadhavani@kpmg.com

Anand Desai
US Financial Services Leader for Risk Services
KPMG LLP
E: ananddesai@kpmg.com

The views and opinions expressed herein are those of the survey respondents and do not necessarily represent the views and opinions of KPMG LLP.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com**