KPMG

Cyber considerations 2025

Financial Services

Foreword

As chief information security officers (CISOs) at financial services organizations embrace digital transformation and cloud adoption, they face several challenges. These include safeguarding critical assets, managing an expanding attack surface, and navigating a complex regulatory landscape. CISOs across the sector must deliver on a broad array of imperatives while operating in a world of reduced visibility and heightened noise due to the proliferation and resulting complexity of data. The capability to focus at once on vulnerabilities, critical assets, and incidents has become critical.

While budgets are not necessarily shrinking, they are also not growing in proportion to increasing demands. CISOs should continuously justify their current spending while struggling to secure additional funding for essentials such as automation and cloud security. The bigger challenge is the tension between focusing budgets on innovative solutions that incorporate artificial intelligence (AI) and machine learning (ML) versus ongoing regulatory remediation given the global uptick in new cyber rules and standards.

In addition, financial services CISOs should also navigate an onslaught of multiregional regulations that are becoming increasingly rigorous and complex. In the US, the Office of the Comptroller of the Currency (OCC) and the Federal Reserve have intensified their oversight of Tier 1 global banks, issuing matters requiring attention, and formal communications from regulators offered during an examination or review that require an institution to address specific issues. Similarly, in the European Union (EU), regulations such as the Digital Operational Resilience Act (DORA), which requires specific tactical security requirements, are increasing in intensity and priority.

To get ahead of these challenges, CISOs are turning to advanced technologies such as AI and ML to automate security operations, reduce false positives, and streamline incident response. However, technology alone is not enough. CISOs need to promote collaboration and ensure their programs align with the objectives of the business by maintaining open communication with senior leaders. Change is already underway. According to KPMG research, 74 percent of financial services organizations say cybersecurity is typically involved from the earliest planning stages of technology investment planning and has a high influence on the decision-making process[1].

In the aftermath of the pandemic, many organizations found themselves with bloated second lines of defense. This eventually led to reassessing existing roles and responsibilities. We encourage CISOs to work closely with the second line of defense—which manages oversight of controls—to focus on operational key performance indicators (KPIs) as proxies of the overall health of the digital environment and align those KPIs with the relevant key risk indicators (KRIs). As always, CISOs must be proactive and adaptable, continuously assessing cybersecurity, identifying gaps, and implementing strong yet flexible controls to mitigate risks.

In this report, we will explore the key cybersecurity considerations for financial services organizations with actionable insights and recommendations for CISOs.

[1] KPMG, Global Technology Report, 2024.

Key cybersecurity considerations for financial services companies in 2025

Key cybersecurity considerations

The power of the people

Embedding trust as AI proliferates

Resilience by design: Cybersecurity for businesses and society

Consideration 1

The power of the people

AI and ML can help financial services firms automate routine cybersecurity tasks, reducing the burden on understaffed teams. With current processes, there is a lot of noise in data, leading to numerous false positives. However, the reality is there aren't enough people to keep up with the volume. AI solutions can help reduce false positives, automatically assign tasks, and escalate important issues to better manage security detections and prioritize and patch vulnerabilities—areas under significant regulatory scrutiny. This can enhance operational efficiency and improve compliance with regulations such as General Data Protection Regulation (GDPR) and Federal Financial Institutions Examination Council (FFIEC).

Key challenges

- **Cyber skills gap**—Financial services firms continue to face a shortage of skilled cybersecurity professionals. This adds to the challenge of addressing the increasing complexity and number of cyber threats.
- **Resource allocation**—Without automation, professionals are consumed by routine tasks. This leaves them less time for addressing and analyzing complex security threats.
- **Regulatory pressure**—Financial institutions are subject to frequently evolving regulatory requirements. Continuously adapting to new standards can be resource intensive and requires careful management to avoid errors.

Key opportunities

- **Enhanced threat detection**—AI and ML provide advanced capabilities for detecting threats, enabling faster and more accurate identification. This can help prevent financial losses and protect sensitive data. Consequently, cybersecurity professionals can dedicate their efforts to more complex and strategic tasks. Indeed, according to KPMG research, 68 percent of financial services professionals agree (24 percent strongly agree) that AI is helping them fill skills gaps among knowledge workers that had previously been a major challenge.[2]
- **Operational efficiency**—Automating routine tasks enables continuous monitoring and rapid data analysis. This leads to faster threat mitigation and better resource utilization. This scalability ensures consistent compliance with cybersecurity regulations and enhances overall resilience.

Many financial organizations recognize the value of using AI and ML in cybersecurity, but adoption varies. Larger institutions currently lead in this regard because of their ability to devote more resources and bring on additional knowledge workers. Smaller organizations lag because of budget constraints. Overall, there is a growing appreciation of the need for automation and readiness to implement these solutions in cybersecurity strategies. Going forward, AI-related disruption will make significant investments in upskilling a strategic imperative, with 40 percent of financial services professionals expecting AI to significantly change job roles over the next 10 years.[3]

[2] KPMG, Global Technology Report, 2024.
[3] KPMG, Global Technology Report, 2024.

Consideration 2

Embedding trust as AI proliferates

The growth of AI offers financial organizations many opportunities to improve operations, customer experience, and innovation. However, it also raises issues of trust, security, and privacy. To maintain data integrity, security, and regulatory compliance, financial institutions embed trust in their AI adoption. Financial services organizations are currently approaching AI governance in a manner similar to model risk management, such as with trading algorithms. In terms of CISO involvement, engagement is not yet sufficient. Many are experimenting with securing AI tools but are uncertain about how these tools differ from other critical data or algorithms.

Key challenges

- **Data privacy and security**—AI systems need large datasets, including sensitive financial information, making them vulnerable to cyberattacks. Financial institutions must navigate privacy and security concerns amid evolving compliance requirements such as GDPR, California Consumer Privacy Act (CCPA) and the EU AI Act.
- **Data quality and bias**—Clean, accurate data is essential for effective AI. Issues with classification, quality, and consistency can cause incorrect or biased outputs. This can damage credibility and lead to decreased trust in AI systems.
- **Transparency and explainability**—Complex AI models, such as deep learning, often function as "black boxes" with limited insight into their decision-making. This lack of clarity can complicate explaining decisions, which is essential for maintaining customer trust and complying with regulations.

Key opportunities

- **Enhanced security through AI**—Using AI and ML for real-time detection and response to security incidents can improve the security measures of financial services organizations. AI can recognize patterns that suggest potential threats. This can allow for faster and more precise responses to cyber threats.
- **Improving data governance and compliance**—Utilizing AI for data governance can help maintain data integrity, accuracy, and compliance with regulatory standards. AI can aid in the automated classification of data, detecting anomalies, and ensuring consistent adherence to privacy regulations. This can promote trust and reliability in AI-driven processes.

Financial services organizations know they must embed trust in AI, but readiness to do so varies. Some currently implement data governance and AI explainability tools, while others lack resources. Awareness of the need for transparency, data quality, and security is growing, with strategies and technologies developing to address these issues.

Consideration 3

Resilience by design: Cybersecurity for businesses and society

With the rise of interconnected systems, cyber resilience in financial services is as crucial as ever. CISOs in this sector must manage a wide attack surface, quickly handle incidents, and maintain resilience practices. In particular, threats to critical infrastructure can significantly disrupt operations and compromise sensitive data. As a result, resilience is now the primary focus of business continuity planning and disaster recovery programs.

Key challenges

- **Extensive attack surface**—The digitization and integration of various systems within financial services have resulted in an expanded attack surface, which presents significant challenges in effectively safeguarding all entry points from potential threats.
- **Quick incident response**—Financial institutions need advanced detection systems and efficient response plans to promptly identify and mitigate incidents.
- **Regulatory compliance and resilience standards**—Financial institutions must follow strict regulatory standards on resilience. These differ based on their significance and interconnections within the financial ecosystem, adding complexity.

Key opportunities

- **Advanced threat detection and response**—Using technologies such as AI and ML, financial institutions can identify and respond to cyber threats more efficiently, reducing potential damage and enhancing overall resilience.
- **Embedding continuous improvement**—Financial institutions can enhance resilience through regular training, advanced technology investments, and proactive attack surface management.

With larger institutions excelling and smaller companies improving, cyber resilience is becoming a second line of defense topic, not just a first-line concern. This is a priority that also extends to critical third parties and cloud providers. Indeed, there is growing scrutiny over what level of disruption to core business functions could ensue if a critical supply chain partner encounters an issue.

Real-world cybersecurity in the financial services sector

In financial services, regulatory requirements are increasingly pressuring organizations to strengthen their vulnerability management capabilities. The overwhelming volume of vulnerabilities and decisions requires an innovative solution to address these risks consistently and systematically.

A leading investment bank was looking to develop and implement AI/ML models that enhance operational efficiency and ensure regulatory compliance. Through close collaboration and a comprehensive assessment of the bank's needs, the KPMG project team devised and deployed ML-driven solutions for vulnerability management and incident response. These solutions leverage targeted use cases to identify weaknesses in current operations and determine where innovative solutions will be most effective. The use cases ranged from triage and ownership assignment to criticality adjustment.

The AI/ML models deployed by KPMG not only reduced manual intervention and accelerated decision-making processes but also incorporated built-in compliance checks. These checks ensured that human expertise maintains proper visibility into the models' decision-making processes, aligning with regulatory requirements.

Such solutions enable financial services organizations to identify, prioritize, and remediate vulnerabilities more rapidly than ever before. Thus, they can tackle a wider range of risks across their entire environment, strengthening their overall cybersecurity posture.

As the sector continues to face mounting pressure from regulatory bodies, organizations that proactively adopt innovative solutions will be better positioned to swiftly identify, prioritize, and mitigate vulnerabilities. By doing so, forward-thinking institutions can not only safeguard their assets and reputation but also stay ahead of the curve in an increasingly complex and demanding cybersecurity landscape.

Top priorities for financial services cybersecurity professionals

- Zero trust architecture: Focusing on identity-centric security and microsegmentation strategies
- Integrating AI/ML-driven tools to automate routine security operations center activities, allowing cybersecurity teams to focus on complex tasks
- Conducting continuous monitoring of third-party vendors to ensure a secure and resilient supply chain
- Developing transparent processes for assessing AI systems, including data classification and quality management, to mitigate privacy concerns and build trust
- Embedding security measures into the development lifecycle of AI technologies to avoid costly retrofitting and potential regulatory or reputational damage
- Engaging with regulatory bodies to stay ahead of compliance requirements and proactively address concerns related to AI implementation

How KPMG professionals can help

With extensive experience in the financial services sector, KPMG firms help CISOs tackle complex challenges, supporting areas such as advanced threat detection, automated incident response, AI-driven vulnerability management, and cyber resilience strategies. We can assist in developing and testing incident response plans, conducting due diligence on third-party vendors, and integrating security into AI technology development. Additionally, we work on regulatory compliance and promote continuous improvement to help ensure operational continuity against evolving cyber threats.

Our commitment to delivering innovative, industry-specific solutions empowers CISOs to proactively address the unique challenges they face and help position their organizations for success in an increasingly complex and demanding cybersecurity landscape. Through our extensive experience and innovative solutions, financial organizations can enhance their cybersecurity posture, protect their assets and reputation, and maintain the trust of their customers and stakeholders.

Contact

Matthew Miller
Principal, Cyber Security Services,
KPMG US
E: matthewpmiller@kpmg.com

Learn more about cyber security services.

KPMG. Make the Difference.

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

Learn about us: **kpmg.com**