KPMG

Fortifying banking cybersecurity:

Strategies

for a resilient future

kpmg.com

Contents

> It is easy to think of cybersecurity as a technology arms race, where the one who spends the most wins."
>
> **Matthew Miller**
> Banking Cybersecurity Leader
> KPMG LLP

Foreward

For a financial services industry advancing quickly into a digital-first future, cybersecurity is critical to safeguarding the interconnected systems, vast stores of data, and customer touchpoints that are emerging.

As institutions shift more and more to digital service ecosystems, they'll need to invest in the people, technology, and expertise necessary to manage threats across an ever-shifting technology estate and ensure enterprise resilience to a growing list of potential disruptors.

The results of the 2025 KPMG Banking Technology Survey illustrate how the industry is responding to the growing demands of protecting operations online. Like last year, institutions are investing in cybersecurity as a top priority as the threat of cyberattacks rises and regulatory demands tighten. "For an industry where stability, security, and privacy are nonnegotiables, cybersecurity will always be front and center on the agenda," said Rahul Jadhav, Financial Services Cyber & Technology Risk Partner, KPMG LLP.

Of the 200 senior bank executives participating in this year's survey, 89 percent named security and fraud prevention a top investment priority over the next 12 months and said they'd be increasing their budgets to address cyber risk. They're also using more automation and managed services for testing to efficiently scale their security management practices.

91% say extra spending is sufficient in cybersecurity protection

Most (91 percent) say this extra spending is sufficient, but it's hard to estimate whether they're doing enough. As threats intensify, banks risk short-changing the cybersecurity efforts needed to protect their critical assets and address regulators on a global scale.

A multinational investment bank transforms security testing capabilities with KPMG

Services

A tier one multinational investment bank and financial services holding company was seeking a trusted MS adviser to provide advanced application security testing capabilities at scale as it struggled to fulfill mandates to test over 1,000 applications annually across the business. Testing needed to meet rigorous internal standards and regulatory requirements.

Methodology

We delivered an extensive support model based on shared services and outcome-based results. Testing included managed application security testing: App penetration testing/API penetration testing, mobile app testing, automated testing (DAST), manual code review, automated code assessments (SAST), operational security assessments, validation assessments.

Benefits

KPMG has provided consistent testing support to the client for four years with a focus on quality and timeliness as key performance indicators. Our commitment to flexibility in service delivery, responsiveness and understanding of the client's challenges (regulatory) has made KPMG their go-to adviser for vulnerability management and application security.

Drivers behind cybersecurity investment

"It is easy to think of cybersecurity as a technology arms race, where the one who spends the most wins," said Matthew Miller, Banking Cybersecurity Leader at KPMG. Instead, proactive cybersecurity management is really an awareness of how technology can both enable business and protect vital assets and operations.

To be successful, banks should consider moving from tick-the-box assessments of security to active management and oversight of the data and services in their supply chain.

From inside and outside this supply chain, they're facing pressure on multiple fronts to put their cybersecurity houses in order. Regulators, for one, are pressing standards and best practices as part of an overall preparedness push for the industry. Others, such as fraudsters, pose direct threats to institutions' stability, profitability, and operational resilience.

Regulators

Country and economic bloc technology frameworks have emerged to promote leading practices and enforce consistent application of soundness and safety standards. Banks should consider adhering to these to protect their customers' sensitive information and support the resilience of the financial system.

Regulatory frameworks such as the General Data Protection Regulation (GDPR) and the Digital Operational Resilience Act (DORA), and standards from entities such as the Office of the Comptroller of the Currency (OCC) and the Federal Reserve, demand stringent security measures, robust risk management practices, and transparent data handling procedures.

Fraud and financial crimes

Fraud and other forms of financial crime are ramping up and evolving, forcing the industry to adapt constantly. Fraud prevention and detection directly impact the integrity, trust, and financial stability of banking operations, so investing in extensive cybersecurity measures to fight fraud is vital.

These days, criminals operate in closely coordinated communities, using new technologies such as artificial intelligence (AI). And while confidence scams and account takeovers aren't cybersecurity issues per se, banks are adding more defensive technology to deter would-be fraudsters, adding to the already long list of priorities for the information security office.

Interestingly, 78 percent of banking leaders in the KPMG survey said GenAI would help facilitate implementation of their security investments this year, a "white hat" application of the technology while criminals increasingly use it to deceive and obfuscate their tactics.

Data protection

The financial services sector maintains highly sensitive and personal data on millions, maybe billions, of consumers. Protecting this data from leakage, breaches, and other forms of data theft is essential to maintaining trust in the industry.

Banks implement a extensive array of cybersecurity measures to protect sensitive data and ensure its confidentiality, integrity, and availability. Given the critical nature of financial information, banks should consider deploying robust security strategies to safeguard against threats.

Operational resilience

Banks invest in technologies, processes, and policies designed to maintain service continuity and quickly recover from disruptions such as DDOS attacks. It underscores the importance of integrating cybersecurity as a core component of banks' resilience planning to protect against and mitigate the impact of cyber threats.

Operational resilience standards also influence banks to develop and regularly test extensive incident response plans that include simulations of cyber incidents. Training staff on these plans is crucial to ensure quick recovery and limit operational disruptions. Regulatory frameworks often mandate operational resilience, requiring banks to demonstrate their preparedness for various disruptions, including cyberattacks.

A multifaceted approach

Banks are strategically investing in multifaceted, extensive cybersecurity measures that enhance their ability to detect and mitigate cyber threats, remain resilient to potential disruptions, and comply with diverse standards and regulations in a fast-evolving digital landscape. "There is no single, magic solution to cybersecurity. Preparation means designing an approach for the whole enterprise, deploying the right tools, and remaining vigilant and adaptive to constantly changing threat conditions," said Charles Jacco, Financial Services Cybersecurity Leader, KPMG LLP.

By investing in leading tools, attracting skilled professionals, and fostering an organizational culture of security awareness, banks aim to protect their operations and maintain trust among customers and stakeholders.

Technology investments

Banks prioritize the deployment of advanced technologies such as AI and machine learning to enhance threat detection, automate security processes, and analyze large datasets for identifying potential vulnerabilities.

They're also investing in robust identity and access management systems, including multifactor authentication and biometric verification, to secure access to sensitive data. Furthermore, banks are enhancing their network and endpoint security through next-generation firewalls, intrusion detection systems and encryption protocols, alongside implementing cloud security tools to protect data in cloud environments.

Expertise through hiring and partnerships

Recognizing the cyber skills gap, banks are investing in attracting and retaining skilled cybersecurity professionals. They collaborate with external cybersecurity firms and technology partners to leverage specialized expertise and advanced solutions. By doing so, banks ensure they have access to the latest threat intelligence and strategic guidance.

Training and awareness programs

Banks invest in comprehensive employee training programs to raise awareness about cybersecurity threats and best practices in data protection. These programs aim to cultivate a culture of security across the organization, enabling employees to identify and mitigate risks effectively. Continuous training initiatives, including workshops and simulations, equip staff to respond to evolving cyber threats and incidents.

As the financial services industry rapidly moves toward a digital-first future, robust cybersecurity measures are critical to preserving the trust, privacy, and reliability on which the industry is built. The strategic investments cited by senior executives in our KPMG 2025 Banking Technology Survey reflect the industry's commitment to maintaining operational resilience, complying with regulatory standards, and building trust with customers. As threats intensify and regulatory demands evolve, banks must continue to prioritize cybersecurity as a core component of their business strategy to navigate an increasingly complex digital landscape.

How KPMG professionals can help

With extensive experience in the financial services sector, KPMG firms helps Chief Information Security Officers (CISOs) tackle complex challenges. We support in 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.

KPMG is a strategic partner on the Cloud Risk Institute's program to strengthen cybersecurity in financial services. It provides technical, research, and advisory support for projects including developing the not-for-profit's Cloud Profile and Cloud Profile Guidebook, the product of a successful collaboration between the private sector and the federal government to create common language, frameworks, and guidance on cybersecurity for the industry.

Our commitment to delivering innovative, industry-specific approaches 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.

KPMG. Make the Difference.

Learn more at https://visit.kpmg.us/bankingtechsurvey

Contact us

Peter Torrente
US Sector Leader—Banking & Capital Markets
KPMG LLP
E: ptorrente@kpmg.com

Charles Jacco
Financial Services Cybersecurity Leader
KPMG LLP
E: cjacco@kpmg.com

Chris Long
Financial Services Advisory Leader
KPMG LLP
E: chrislong@kpmg.com

Matthew Miller
Banking Cybersecurity Leader
KPMG LLP
E: matthewpmiller@kpmg.com

Rahul Jadhav
Financial Services Cyber & Technology Risk Partner
KPMG LLP
E: rjadhav@kpmg.com

Andrew Ellis
Banking Advisory Leader
KPMG LLP
E: alellis@kpmg.com

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**