



Unraveling five essential cybersecurity priorities for banks

Cyber threats are a persistent top risk in banking. CISOs can be more effective at addressing them.



In the increasingly digital world of banking, cybersecurity has shifted far beyond the technological or risk management realm. It is a fundamental strategic capability, necessary for building brand trust, harnessing the potential of emerging technologies, innovating new digital features and offerings, and complying with the growing privacy and security demands of customers and regulators. The [2024 U.S. Banking Industry Outlook Survey](#) found that cybersecurity risk poses the greatest threat to growth, ahead of all other risks.¹

Cyber risk remains a top industry issue despite the fact that privacy and security are not underprioritized in most banks, at least based on the numbers. Our research shows that most bank leaders are well aware of the competitive urgency to bring down cyber risk and are investing accordingly. Although 78 percent of executives believe their bank already has adequate cybersecurity and data protection, more than half (55 percent) are nonetheless increasing their budget to address cyber risk.² And many are being fast and agile in their cyber investments, with 60 percent having already piloted newly emerging generative artificial intelligence (GenAI) cybersecurity solutions.³



Cybersecurity is well known as a strategic imperative in the banking industry, but awareness hasn't translated to sufficient risk reduction. Relentless cyber threats remain a foremost threat to bank growth, requiring CISOs to really hone in on the most difference-making security capabilities.

Matthew Miller, US Financial Services
Cyber Security Leader, KPMG LLP



Cybersecurity risk is the top threat to growth in banking



Cybersecurity is the most common GenAI active use case in the banking industry

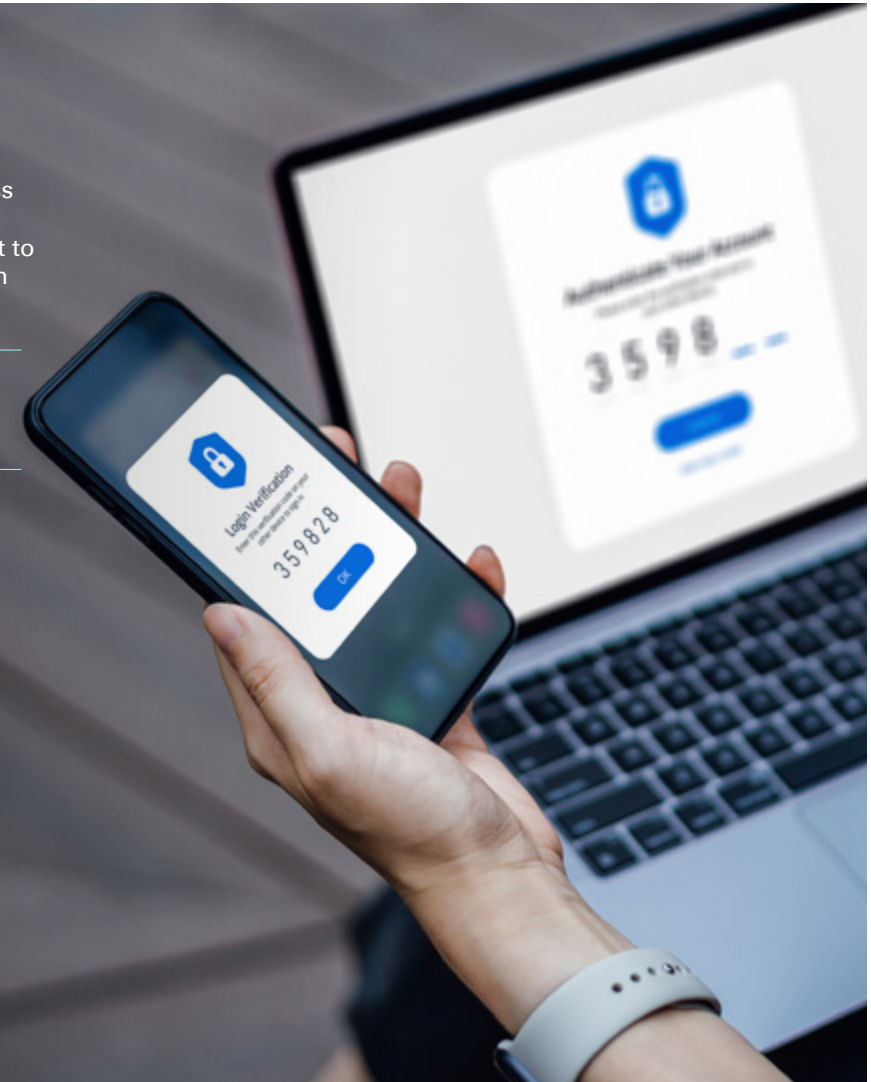


55% are increasing their budget to address cyber risk

¹ KPMG LLP, "2024 KPMG U.S. Banking Outlook Survey," 2024

² *ibid*

³ *ibid*

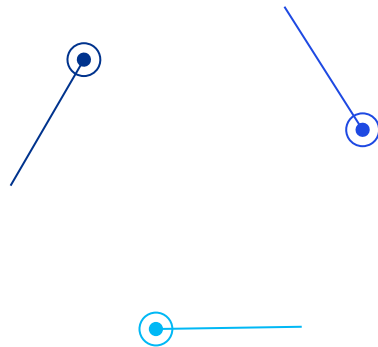




Why the fear persists

From the outside, it might look like most banks should have the resources they need to protect against cyberattacks and data breaches, reduce the risk of cyber incidents, and prepare themselves for evolving cyber threats. But inside, chief information security officers (CISOs) and their security teams know differently.

Cyber risk is a stubborn beast. Despite more spending and steady progress, it remains a top industry concern and an unaddressed risk area. Several trends are driving forces behind the relentless cyber risks faced by the banking industry.





KPMG helps CISOs prioritize five urgent cybersecurity needs in banking

Clearly, cyber risk in banking isn't going away. But getting better at addressing it is essential for banks' survival today and success tomorrow. Cyberattacks can result in financial losses through direct costs (remediation, legal fees) and indirect costs (lost revenue from outages, tech debt, lost customers, brand reputation damage, and decreased stock price). Research found that cybercrime cost \$8 trillion in 2023 and is expected to rise to a staggering \$10.5 trillion by 2025.⁷

As a leading cybersecurity adviser to banks and other financial institutions, we understand the critical issues that have kept cybersecurity as such a persistent and significant risk in the industry. We help CISOs cut through the complexity of this fast-evolving space with a suite of market-leading solutions that are based on the five most pressing cybersecurity needs in banking.

⁷ USA Today, "Cybersecurity statistics in 2024," March 27, 2024



Connect with us

Whether you're entering a new market, launching products and services, or interacting with customers in a new way, KPMG can help your bank improve cybersecurity posture and capabilities now and for the future. Please visit <https://kpmg.com/us/en/capabilities-services/advisory-services/cyber-security-services.html> or reach out to start a conversation.

Matthew Miller
US Financial Services Cyber Security Leader
KPMG LLP
matthewpmiller@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS014454-1E