THE STATE OF CYBERSECURITY

Emerging threats and trends in financial services

How banks, investment firms, and fintechs can stay ahead of cyber risks

KAUFMAN ROSSIN

Learn more at kaufmanrossin.com

EXECUTIVE SUMMARY

The financial services industry is facing an unprecedented level of cyber risk.

As digital transformation accelerates and technology use continues to evolve, banks, investment firms, and fintech companies are grappling with new challenges. While artificial intelligence (AI) and other technologies provide significant benefits, they also introduce new cyber risks, with cybercriminals leveraging increasingly sophisticated tactics to exploit vulnerabilities, disrupt operations, and steal valuable data.

Cyberattacks have grown in both volume and complexity – and the impact has increased exponentially. According to IBM's 2024 report, the average cost of a data breach globally is now $4.88 million, while in the United States, this number rises to $9.36 million. The consequences of these attacks extend far beyond financial losses, posing operational, reputational, and regulatory risks that can significantly impact an organization's long-term success.

To stay ahead of these evolving threats and stay compliant with industry regulations, financial services firms should take a proactive approach to cybersecurity, focusing on threat intelligence, AI-powered defenses and employee training. This report explores some of the most pressing cyber threats facing the financial services industry today and outlines best practices to strengthen cybersecurity resilience.

EVOLVING CYBER THREAT LANDSCAPE

The global financial services market is expected to see strong growth in the coming years, rising from $31.14 trillion in 2023 to $44.93 trillion in 2028, per Research and Markets.

This growing sector has long been a prime target for cybercriminals due to its vast collection of sensitive customer and financial data, high transaction volumes, and reliance on interconnected digital networks. A 2024 report by the International Monetary Fund (IMF) noted that nearly one in five reported cyber incidents worldwide has affected financial institutions.

44.28%

Projected growth for the global financial services market from 2023 ($31.14 trillion) to 2028 ($44.93 trillion)

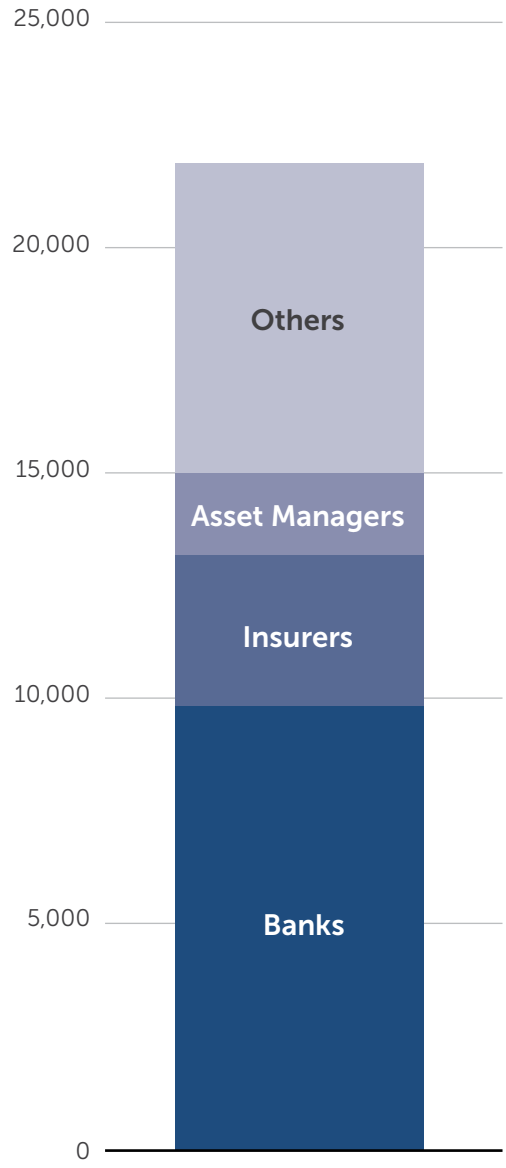
Further, the IMF notes that cyber threats in the financial sector have accelerated rapidly, with $12 billion in direct losses recorded over the past two decades. IMF warns that these incidents pose a serious risk to global financial and economic stability, especially if they "erode confidence in the financial system, disrupt critical services, or cause spillovers to other institutions."

Regulators are looking at financial institutions' operational resilience, third-party risk management, and risks related to emerging technology. With banks, investment firms, and fintechs operating in a high-risk, high-stakes environment and regulators intensifying their scrutiny of cybersecurity practices within the financial industry, the imperative for strong cybersecurity measures has never been greater.

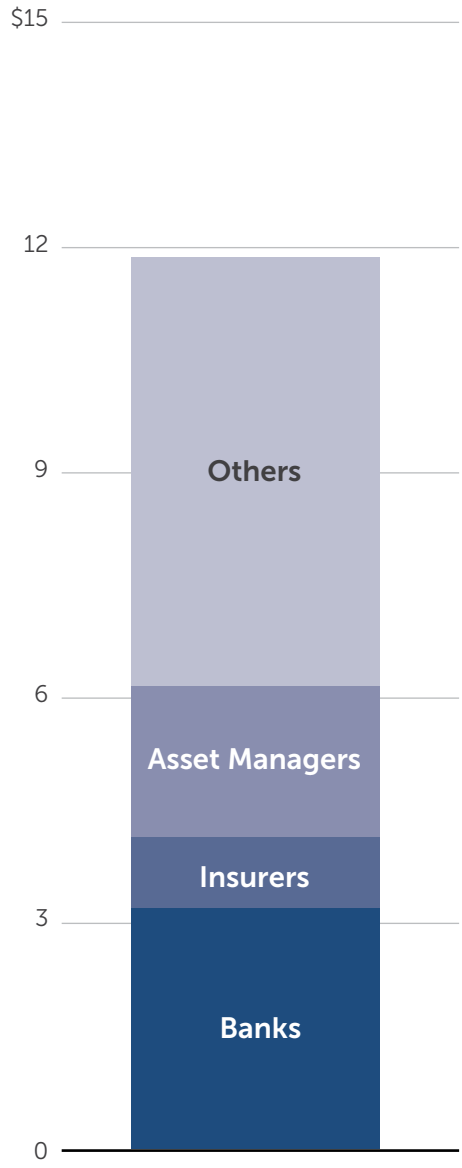
Attractive target

The financial sector has suffered more than 20,000 cyberattacks, causing $12 billion in losses, over the past 20 years.

Financial sector cyber incidents
(number, 2004-23)



Financial sector losses
(billions of U.S. dollars, 2004-23)



Source: Advisen cyber loss data and IMF staff calculations, IMF

EVOLVING REGULATORY LANDSCAPE

Financial industry regulators are paying close attention to growing risks associated with new technologies, emerging threats, and third-party relationships. In some cases, they are issuing new guidance or adopting updated standards. Regulations around AI, for example, are still evolving. Several countries and international organizations are working on frameworks and guidelines for ethical, safe and responsible use of AI.

The FFIEC announced that it will be sunsetting the 10-year-old Cybersecurity Assessment Tool (CAT) after August 2025. Instead, the FFIEC is encouraging financial institutions to use one of the newer tools in assessing their cybersecurity program. Leading cybersecurity frameworks include the National Institute of Standards and Technology Cybersecurity Framework 2.0, the Cyber Risk Institute (CRI) Profile 2.0, and the Cybersecurity and Infrastructure Security Agency's Cybersecurity Performance Goals.

The landscape of third-party risk management is rapidly evolving as cyber threats continue to grow in sophistication. In July 2023, U.S. financial regulators issued Interagency Guidance on Third Party Relationships: Risk Management, which provides principles for financial institutions to follow in support of a risk-based approach to third-party risk management. That guidance was followed in December 2023 with the Financial Stability Board's tool kit for enhancing third-party risk management and oversight. Financial institutions should stay up-to-date on these evolving standards and implement comprehensive risk management programs that address the dynamic and interconnected risks posed by third-party relationships.

Both FINRA and the SEC have emphasized the importance of cybersecurity for investment firms over the past few years. In July 2023, the SEC adopted final rules requiring firms to "disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance."

TOP & EMERGING CYBERSECURITY THREATS

Cybercriminals are continually adapting their strategies, using tools like AI, credential stuffing, and phishing to launch more sophisticated and harder-to-detect attacks. Some of the most impactful cyber incidents in recent history occurred in the past year alone, exposing the vulnerabilities that persist within the industry.

1 Phishing, vishing, and social engineering attacks

Among the most persistent cybersecurity threats in financial services are phishing, vishing (voice phishing), and social engineering attacks. These methods remain highly effective because they exploit human error, tricking employees, customers, and executives into revealing sensitive information (e.g., credentials) or approving fraudulent transactions.

According to Verizon's 2024 Data Breach Investigations Report, 68% of breaches involve the human element, with phishing and impersonation scams playing a major role. The sophistication of these attacks has increased with the use of AI-generated content. Deepfakes, for example, allow cybercriminals to impersonate executives in real-time, manipulating victims into transferring funds or disclosing critical information.

In one case reported by CNN, a finance worker at a multinational firm transferred more than $25 million to fraudsters after being tricked by a deepfake video call impersonating the company's chief financial officer.

2 AI and Machine Learning (ML)-driven cyber threats

As financial institutions embrace AI/ML technology to enhance the user experience and bolster cybersecurity defenses, cybercriminals are finding new and innovative attack vectors to infiltrate networks and compromise data.

For example, cybercriminals are using AI to:

- Enhance malware to bypass traditional security measures
- Launch automated, adaptive phishing campaigns based on user behavior
- Break CAPTCHA systems and compromise customer accounts through credential stuffing

AI-driven cyber fraud is another growing concern, especially as deepfake technology is being used by criminals to create fake identification and submit fraudulent loan applications and insurance claims. In the fintech sector alone, deepfake incidents shot up 533% in Q1 2024 from Q1 2023, according to Sumsub, an identity verification platform provider.

> *"As the technology evolves, the difference between synthetic media and human-generated content is becoming harder to discern even for detection technologies, making deepfakes more realistic, more targeted and dangerous than ever before."*
>
> **– World Economic Forum**

3 Ransomware attacks

Ransomware remains a significant threat, with attackers encrypting organizations' critical data and demanding hefty ransom payments to restore access. These attacks can cripple financial services firms, halting operations and exposing sensitive customer information. It's also important for organizations to understand that there is no guarantee that attackers will release their data once a payment is received.

In June 2024, a commercial bank disclosed a ransomware attack in which a hacking group demanded a $1 million ransom after stealing employee data. A 2023 ransomware attack on a cloud IT service provider caused more widespread disruption, triggering simultaneous outages at 60 credit unions, per the National Credit Union Administration (NCUA).

4 Third-party vendor risks

Financial institutions are increasingly relying on third-party providers for cloud services, payment processing, and IT infrastructure. However, these external vendors can introduce supply chain vulnerabilities, allowing cybercriminals to exploit a single weak link to compromise multiple organizations.

In March 2024, a bank holding company notified its cardholders regarding a potential data breach stemming from a third-party payment processor widely utilized by numerous merchants. The notices warned the breach may have compromised customer payment details such as names, card numbers, and expiration dates.

5 Cloud services

Financial services firms are increasing their adoption of cloud technology for improved resilience and the introduction of new capabilities. However, it's imperative to properly manage the associated risks that come with increasing reliance on the cloud.

Misconfigurations, incomplete data deletion and inadequate access controls are some of the most common issues that lead to unauthorized access and data breaches.

CYBERSECURITY DEFENSE AND BEST PRACTICES

Financial institutions will need to implement more robust systems and processes to detect and respond to growing cyber threats, especially as AI-driven attacks become more prominent. Fortunately, AI can also be used to help detect and address threats.

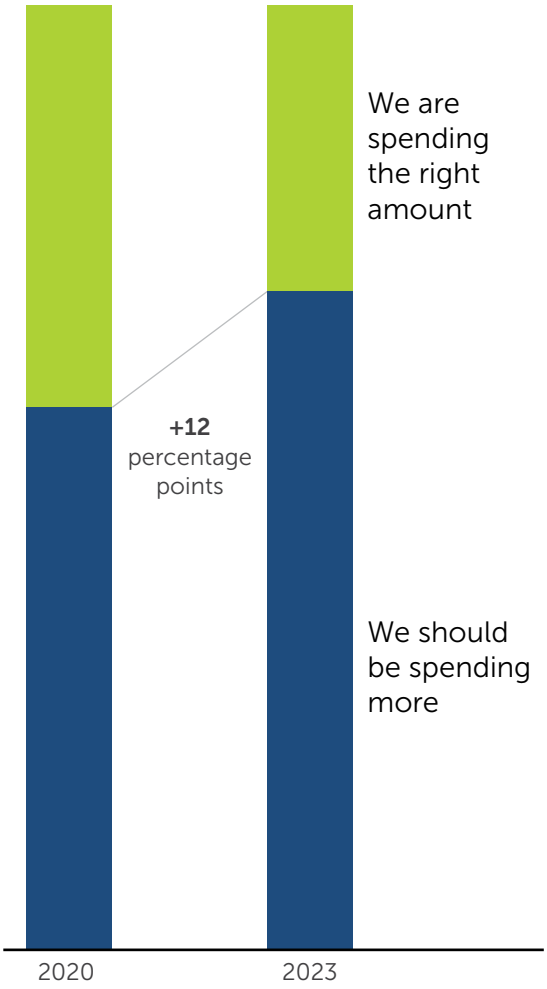
The 2024 IBM study found that participants who used AI and related technologies in cyber threat detection reported substantially lower data breach costs and faster detection times. This finding suggests that leveraging AI as a tool to combat cyber threats is no longer an aspirational idea, but a key consideration for financial services firms.

> *"When deployed extensively across prevention workflows—attack surface management (ASM), red teaming and posture management—organizations averaged $2.2 million less in breach costs compared to those with no AI use in prevention workflows."*
>
> **– IBM**

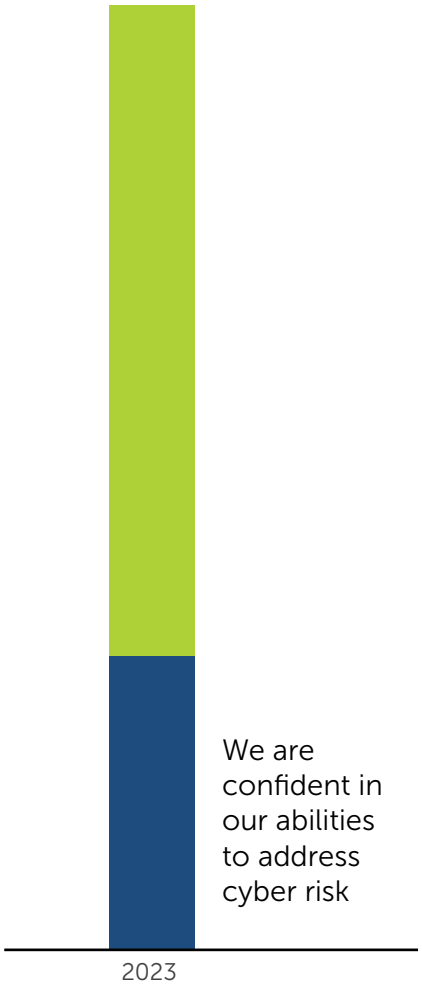
Cybersecurity spending

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

Spending on cybersecurity[1]
% of respondents (n = 37)



Cybersecurity confidence[2]
% of respondents (n = 37)



[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: McKinsey & Company

1 Implementing Zero Trust security

A growing number of financial institutions are adopting Zero Trust security models, which assume that no user or device should be trusted by default. Zero Trust is a security model that aims to reduce the risk of unauthorized access and data exposure. The motto of Zero Trust is "never trust, always verify". This means that every user, device, and network should be verified at every step.

The Zero Trust approach:

- Requires continuous identity verification
- Limits user access based on least privilege principles
- Uses real-time threat detection to flag suspicious activity

2 Leveraging AI for threat detection

As much as AI and ML pose new cyber risks, this technology also presents new solutions and capabilities to enhance cybersecurity programs and defend against threats. It can assist in risk assessment, threat detection and prevention, automated incident response, and behavioral analysis.

Global data and business intelligence provider Statista projects that AI spending in the financial sector will increase from $35 billion in 2023 to over $126 billion by 2028, highlighting its growing role in cybersecurity.

AI / ML technology can improve an organization's cyber posture and help prevent fraud and identify theft by identifying patterns, detecting anomalies and responding to threats in real-time. This might include using advanced AI systems to analyze behavioral patterns, voice intonations or visual inconsistencies in video or audio.

> *"Zero Trust essentially means that no device or user should ever be afforded default access to any application, system or digital asset. If you start by keeping everything shut off and only turning on access as needed via authentication and authorization, you can limit unauthorized users from accessing sensitive data."*
>
> **– Jeff Bernstein,** Kaufman Rossin

3 Enhancing employee training and phishing awareness

Humans are the weakest link in security. Employee education, such as training team members to use strong passwords and recognize possible attacks, is crucial in combatting social engineering threats. The better employees understand the behaviors, tactics and techniques of threat actors, the better prepared they will be to identify and mitigate a potential incident.

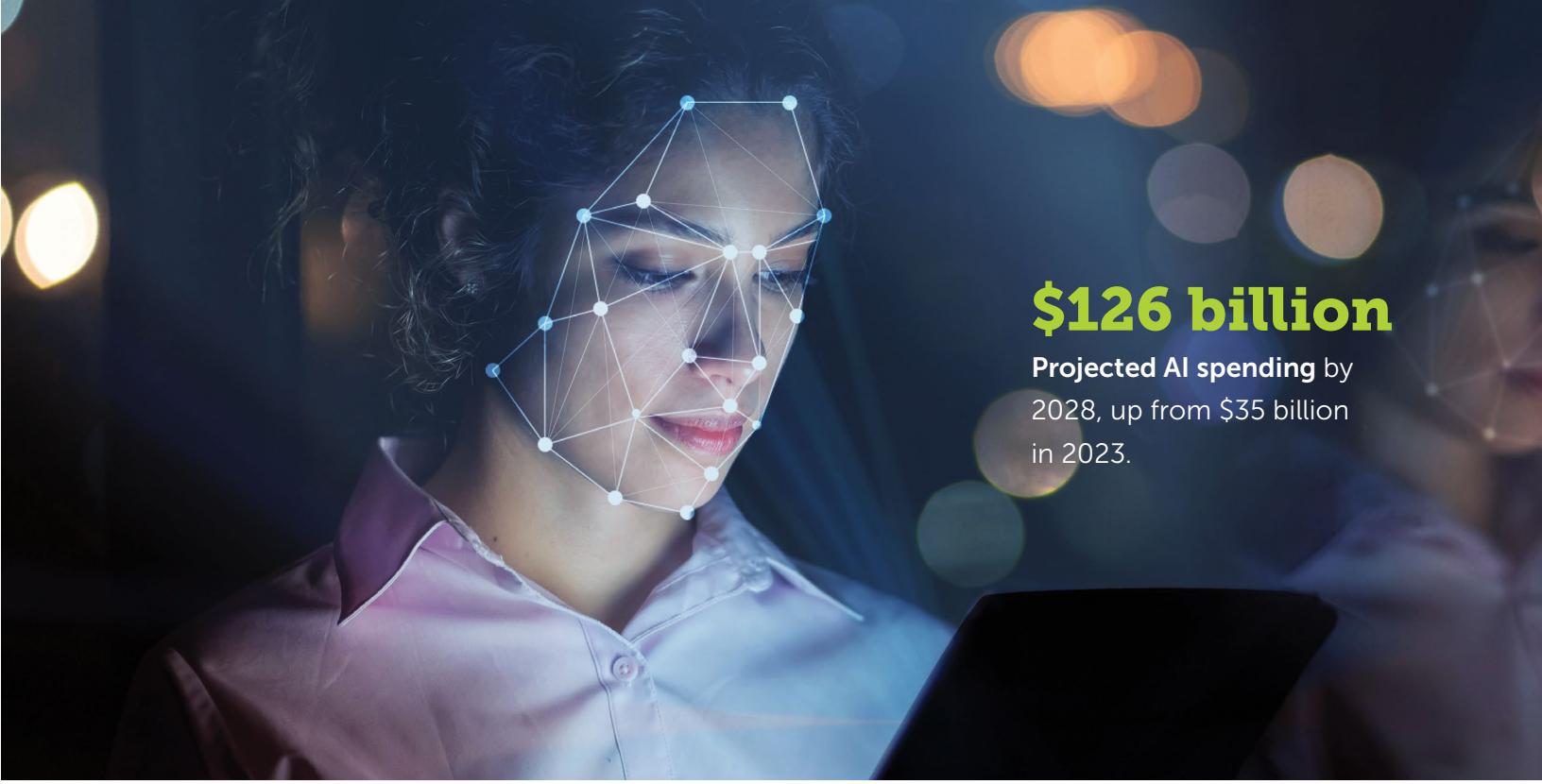
This is especially important because phishing attacks are usually just the tip of the spear for cybercriminals. Hackers often leverage phishing to access systems, install malware or launch ransomware attacks, amplifying the damage to the organization.

4 Encryption and tokenization

Data encryption and tokenization are both methods that can be used by financial services firms to help protect sensitive data.

Encryption scrambles the original data into an unreadable format using a key, while tokenization replaces the sensitive data with meaningless placeholders called "tokens," making it significantly harder for attackers to use even if compromised. There is no key or algorithm that can be used to derive the original data for a token. Instead, tokenization uses a database, called a token vault, which stores the relationship between the sensitive value and the token. The real data in the vault is then secured, often via encryption.

Essentially, encryption hides the data, while tokenization removes the original data and replaces it with random data.



5 Other best practices

The cyber strategy and risk management practices are underpinned by effective governance. Financial service firms should practice robust risk management, both inside and outside the organization.

This includes using Multi-Factor Authentication (MFA) to add an extra layer of security by requiring users to provide two or more forms of verification when authenticating – typically something they know (a password), something they have (a smartphone or token), and / or something they are (biometrics). When paired with Single Sign On (SSO), it can improve security and user experience through streamlined authentication.

It also includes following industry standards and best practices around firewalls, attack surface management, threat monitoring and vulnerability scanning, cybersecurity policies and procedures, regular data backups, and business continuity and incident response plans.

CONCLUSION

Preparing for the future of cybersecurity

As cyber threats evolve, financial institutions, investment firms and fintechs must remain vigilant in securing their digital assets, customer data, and operational infrastructure. They should revisit their cybersecurity policies and practices on an ongoing basis and be ready to adapt to the changing nature of threats.

Adopting proactive and adaptive cybersecurity measures, such as AI-driven solutions, periodic risk and vulnerability assessments, penetration testing, and employee training and testing will be essential to defending against increasingly sophisticated cyber risks.

Financial services firms should also consider engaging a cybersecurity consultant to assist with cyber readiness, including assessing current and future risks, implementing risk mitigation strategies, and responding to any cyber incidents that may occur.

> *"Many enterprises reach a point where in-house capabilities cannot keep up with the threats to their networks, applications, systems, data, devices, people, and property. Furthermore, gaps in employee awareness or vetting of vendors are an open invitation to cybercriminals to steal valuable data."*
>
> **– Kanishk Mehta,** Kaufman Rossin

WANT TO LEARN MORE?

Kaufman Rossin offers a full suite of cybersecurity risk management solutions, within our TRACS framework (Training, Response, Assessments, Compliance, and SOC reports). We provide industry leading solutions, including risk assessments, deepfake simulations, digital transformation, process re-engineering, and phishing simulation training to help banks, investment firms and fintechs mitigate cyber threats.

Contact us to learn more about how our cybersecurity professionals can help your organization stay ahead of emerging cyber risks.

Jorge Rey
Principal, Cybersecurity and Compliance
jrey@kaufmanrossin.com

Kanishk Mehta
Director, Risk Advisory Services
kmehta@kaufmanrossin.com

Jeffrey Bernstein
Director, Cybersecurity and Data Privacy
jbernstein@kaufmanrossin.com

KAUFMAN

ROSSIN