The CRO's Sense Guide to Cyber Security Threats in 2025.

A subject aid for non-SME financial services risk managers on navigating the complex topic of cyber-security threats.

Owen Vallis

2025-01-21

Contents

Introduction

I'm not a cyber-security subject matter expert, I am a holistic Risk Manager with a diverse and generalised skilset.

In the time that cyber-security has come under my remit as a Chief Risk Officer, I've found that one of the main challenges is translating technical cybersecurity threats into actionable insights for our boards, executive teams, and risk committees. This document has been crafted with that specific challenge in mind.

In my twenty years of risk management experience, I've never seen a threat landscape evolve as rapidly as it has in recent months. The emergence of AI-powered attacks, combined with geopolitical tensions and the continued digitalisation of our industry, has created a perfect storm that demands our immediate attention and understanding. The purpose of this analysis is not to overwhelm you with technical details, but rather to provide you with the strategic context needed to:

- Engage meaningfully with your technical teams
- Anticipate questions in risk committee meetings
- Make informed decisions about resource allocation
- Communicate effectively with your board about emerging threats
- Develop credible and relevant scenarios for operational resilience, regulatory reports, and table-top excercises.

As CROs, we often find ourselves bridging the gap between technical experts and business leaders. This can be particularly challenging in cybersecurity, where the technical complexity can obscure the business implications of emerging threats. I've structured this document to help you navigate these conversations with confidence.

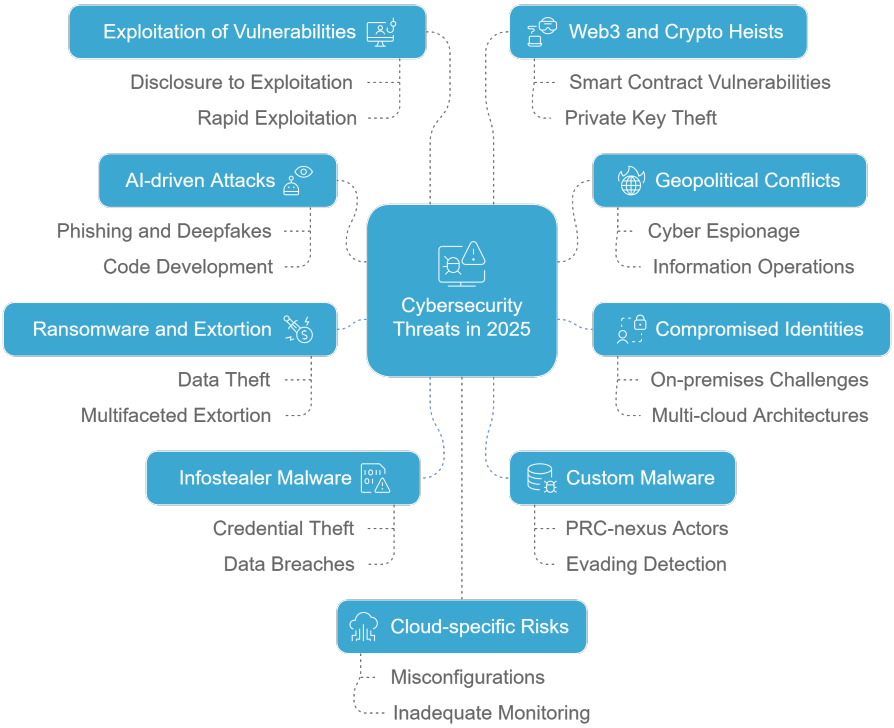
When reviewing this document, I encourage you to focus on three key questions:

- How would these threats specifically impact your institution's business model?
- Are your current risk identification and assessment frameworks adequate to evaluate these emerging threats?
- Do your mitigation strategies align with both your risk appetite and operational capabilities?

You'll notice that I've assigned priority levels to each threat. These are based not just on technical severity, but on the broader business impact and the complexity of mitigation. Use these as a starting point for your own risk prioritisation discussions, adapting them to your institution's specific context.

A word of caution: while this document aims to be timely and relevant, the threat landscape is dynamic. I strongly recommend establishing regular review cycles with your security teams to update and refine your understanding of these threats as they evolve. For those of you who, like me, didn't come from a technical background, I've made a particular effort to explain complex concepts in business terms. Use this document as a foundation for deeper discussions with your technical teams, who can provide institution-specific context and technical details. Remember, our role is not to be cybersecurity experts, but rather to ensure that cybersecurity risks are properly understood, evaluated, and managed within our institutions' broader risk management frameworks. The following analysis represents our best current understanding of the threats we'll face in 2025. I encourage you to read it not just as a risk assessment, but as a strategic planning tool that will help you engage more effectively with all stakeholders in your organisation's cybersecurity environment.

Top Cyber-Security Risks for 2025



AI-Driven Attacks

Priority Level: 1 (Critical)

Artificial Intelligence has emerged as a transformative force in the cybersecurity landscape, with malicious actors leveraging advanced language models and deep learning capabilities to create increasingly sophisticated attack vectors. These AI-powered tools have dramatically enhanced the precision and scalability of traditional cyber threats, while simultaneously lowering the technical barriers for conducting complex attacks.

> Artificial Intelligence (AI):
>
> The use of computers and software to perform tasks that usually require human intelligence, like recognising patterns, making decisions, or mimicking human behaviors.

Within the financial sector, this technological evolution has manifested in deeply concerning ways. Financial institutions now face AI-enhanced attacks that demonstrate unprecedented levels of sophistication in mimicking legitimate banking communications and processes. These systems can analyse patterns

in financial communications and customer service interactions to generate highly convincing fraudulent content that easily bypasses traditional detection methods. The automation capabilities of AI have also enabled attacks to scale dramatically, allowing threat actors to simultaneously target thousands of customers with personalised, contextually aware social engineering campaigns.

> Social Engineering:
>
> A method used by attackers to trick people into giving away sensitive information, like passwords, by pretending to be someone they trust.

Customers of financial institutions face particularly acute vulnerabilities in this new landscape. The emergence of sophisticated voice cloning technology has made it possible for attackers to impersonate both banking representatives and customers themselves, leading to a surge in fraud incidents. AI-driven synthetic identity creation has also become remarkably sophisticated, combining multiple data points to create convincing false identities that can withstand traditional verification processes.

> Real-World Example:
>
> Voice Cloning Incident leads to $35 million loss (2020) Voice cloning technology was used to impersonate a company executive in an massive fraud scheme. The incident highlights the emerging threat of AI-powered social engineering. Source: Forbes

Geopolitical Cyber Operations

Priority Level: 1 (Critical)

The intersection of geopolitical tensions and cyber capabilities has created a new battlefield where financial institutions often serve as primary targets. Nation-state actors are increasingly viewing cyber operations against financial targets as a crucial tool for achieving strategic objectives, whether through direct system disruption or more subtle forms of economic manipulation.

The impact on financial institutions has been profound and far-reaching. These sophisticated actors are targeting core financial infrastructure with unprecedented precision, seeking to disrupt international payment systems during critical periods of geopolitical tension. Beyond direct disruption, there's a growing trend of state-sponsored espionage targeting proprietary trading algorithms and market positions, potentially undermining the integrity of financial markets themselves.

Identity Compromise in Hybrid Environments

Priority Level: 1 (Critical)

The modern financial institution's technology infrastructure represents a complex web of interconnected systems spanning traditional on-premises deployments and multiple cloud environments. This hybrid architecture, while offer-

ing operational benefits, has created new challenges in maintaining consistent identity security across diverse technological boundaries.

In this environment, compromised credentials have become particularly dangerous, as they can serve as a gateway for lateral movement across multiple systems and platforms. Financial institutions are grappling with the challenge of maintaining secure identity management across environments where traditional security perimeters have essentially disappeared. The compromise of a single identity can now cascade through interconnected systems, potentially affecting everything from trading platforms to customer data repositories.

Ransomware and Multifaceted Extortion

Priority Level: 2 (High)

> Ransomware:
>
> A type of malicious software that locks your files or systems until you pay the attacker a ransom, often in cryptocurrency.

The evolution of ransomware has transformed what was once a straightforward encryption-for-payment scheme into a sophisticated multi-stage attack methodology. Modern ransomware operators now employ a strategic combination of system encryption, data theft, and public pressure tactics, creating layered extortion scenarios that pose complex challenges for financial institutions.

The impact on financial institutions manifests in particularly concerning ways. Beyond the immediate operational disruption of encrypted systems, institutions face the compound threat of sensitive financial data exposure. Trading systems, once compromised, can result in market disruption and significant financial losses even if restored quickly. The reputational damage from these attacks can be especially severe in the financial sector, where customer trust is paramount and regulatory scrutiny is intense.

Customers of affected institutions often face cascading consequences. The inability to access banking services during an attack can lead to missed payments, failed transactions, and financial hardship. More concerning is the potential exposure of personal financial information, which can lead to long-term implications for customers' financial security and privacy.

Infostealer Malware

Priority Level: 2 (High)

> Infostealer Malware:
>
> A type of malicious software designed to secretly steal sensitive information like passwords, financial data, or personal details.

Information-stealing malware has evolved into highly sophisticated toolsets specifically designed to target financial data and credentials. These modern

infostealers employ advanced techniques to evade detection while harvesting sensitive information from both institutional systems and customer devices. Their ability to operate silently while gathering critical financial data makes them particularly dangerous in the banking sector.

Financial institutions face the challenge of protecting against malware that specifically targets their employees' credentials and access tokens. These attacks often focus on gathering login information for critical financial systems, trading platforms, and customer databases. The sophisticated nature of modern infostealers means they can persist undetected for extended periods, gradually accumulating sensitive data that can be used for future attacks.

Customer impact from infostealer malware is particularly severe in the financial sector. Personal banking credentials, once harvested, can lead to unauthorised transactions and account takeovers. Cryptocurrency owners face additional risks, as specialised malware variants specifically target digital wallet credentials and private keys. The interconnected nature of modern financial services means that compromised credentials can affect multiple accounts and services simultaneously.

Rapid Vulnerability Exploitation

Priority Level: 2 (High)

The window between vulnerability discovery and exploitation has shrunk dramatically, putting unprecedented pressure on financial institutions to maintain security across complex technology stacks. Threat actors are increasingly capable of weaponising new vulnerabilities within hours of their disclosure, sometimes even before patches are available.

Financial institutions must now manage an accelerated security response cycle while maintaining the stability of critical systems. The challenge is particularly acute in trading and transaction processing systems, where downtime for patching can have significant financial implications. The complexity of modern financial technology stacks, often involving multiple third-party integrations, makes comprehensive and rapid vulnerability management especially challenging.

Customer-facing systems present particular concerns in this rapid exploitation environment. Mobile banking applications and online banking platforms must be constantly updated to address new vulnerabilities, while maintaining functionality and user experience. The exposure of customers to unpatched vulnerabilities can lead to account compromise and financial losses.

Cloud Security Risks

Priority Level: 2 (High)

The financial sector's accelerating migration to cloud services has created a complex security landscape where traditional perimeter-based security approaches no longer suffice. Cloud environments introduce unique challenges around data sovereignty, shared responsibility models, and the dynamic nature of cloud resources. The complexity is further amplified by the adoption of multi-cloud

strategies, where institutions leverage different cloud providers for various services.

Financial institutions face significant challenges in maintaining security across their cloud infrastructure. Misconfigurations, particularly in complex multi-cloud environments, can lead to catastrophic data exposures. The dynamic nature of cloud resources means that security controls must be continuously monitored and updated. Authentication systems spanning multiple cloud providers create additional complexity in managing access controls and preventing credential abuse.

> Real-World Example:
>
> Microsoft Cloud Platform Breach (2023) Hackers compromised Microsoft's cloud infrastructure, potentially affecting email systems of multiple financial institutions. Source: Microsoft

For customers, the implications of cloud security risks are far-reaching. Their financial data, now distributed across various cloud environments, faces exposure risks from misconfigured storage systems or inadequate access controls. The interconnected nature of cloud-based banking services means that a security breach in one system can potentially compromise multiple services simultaneously. Mobile banking applications, which heavily rely on cloud infrastructure, become particularly vulnerable to service disruptions or data breaches resulting from cloud security incidents.

Democratisation of Cyber Capabilities

Priority Level: 2 (High)

The increasing availability of sophisticated cyber attack tools and services has dramatically lowered the barrier to entry for cybercrime targeting financial institutions. This democratisation of cyber capabilities means that advanced attack techniques, once limited to nation-state actors, are now accessible to a broader range of threat actors. The emergence of Cybercrime-as-a-Service (CaaS) platforms has created a sophisticated underground economy where attack tools and services can be easily purchased and deployed.

The impact on financial institutions is particularly concerning as they now face attacks from a larger and more diverse set of threat actors. These actors range from sophisticated cybercrime groups to opportunistic individuals using purchased attack tools. The standardisation and commoditisation of attack methods have made it harder to attribute attacks and develop effective countermeasures. Financial institutions must now defend against both highly sophisticated targeted attacks and a rising volume of automated, tool-based attacks.

Customer vulnerability has increased significantly with this democratisation of attack capabilities. Fraudsters can now purchase sophisticated phishing kits specifically designed to target banking customers, complete with artificial intelligence-powered features for evading detection. The availability of automated account takeover tools has made it easier for attackers to compromise customer accounts at scale. Social engineering scripts and attack methodologies

specifically designed for financial fraud are readily available on underground markets, leading to more convincing and effective scams targeting banking customers.

Custom Malware for Embedded Systems

Priority Level: 3 (Moderate)

The financial sector's reliance on specialised embedded systems has created a unique attack surface that threat actors are increasingly targeting with custom-designed malware. These bespoke threats are specifically engineered to exploit the particular vulnerabilities of financial infrastructure, from ATM networks to trading terminals.

For financial institutions, the impact of custom malware targeting embedded systems extends beyond immediate operational disruption. ATM networks, once compromised, can be manipulated to dispense cash or collect card data. SWIFT terminals and other critical financial messaging systems can be compromised to initiate fraudulent transactions or manipulate financial records. The specialised nature of these systems often means that traditional security tools are less effective at detecting and preventing these custom attacks.

Customers experience the effects of these attacks through compromised ATM transactions, skimmed card data, and potential exposure of their financial information through infected point-of-sale systems. The sophisticated nature of custom malware means that customers may be unaware of the compromise until fraudulent activities appear in their accounts.

Web3 and Crypto Attacks

Priority Level: 3 (Moderate)

The integration of cryptocurrency and decentralised finance (DeFi) services into traditional banking has created new attack vectors that bridge conventional and digital finance. Smart contract vulnerabilities, custody solution compromises, and cross-chain bridge attacks represent complex technical challenges that many financial institutions are still learning to address.

For financial institutions offering crypto services, the impact of these attacks can be severe and immediate. Smart contract exploits can lead to significant financial losses, while compromises in custody solutions can affect both institutional and customer assets. The reputational damage from crypto-related incidents can be particularly severe, as this technology is still viewed with skepticism by many traditional banking customers.

Customers engaged in crypto services through their financial institutions face risks from both technical vulnerabilities and sophisticated scams. Smart contract exploits can result in the loss of digital assets, while vulnerabilities in wallet integration systems can expose traditional banking credentials. The complexity of these systems makes it particularly challenging for customers to understand and protect against these risks.

So What's Next?

Risk Culture

As the CRO, and a non-SME in cyber-security, promoting a high-quality Risk Culture around cyber-security will be the area where you can make an outsized impact. While technical controls and security frameworks provide essential protection, the human element remains both the greatest vulnerability and the strongest potential defense against cyber threats. Leave the technical monitoring and management to the specialist teams, and focus your efforts on managing the human element throughout you organisation, using your visible profile as CRO to promote positive cultural change.

Leadership's Role in Cultural Transformation

The journey toward a strong cybersecurity risk culture begins at the top. Board members and executives must do more than merely endorse security initiatives – they must actively embody the security-first mindset they wish to instill throughout the organisation. This involves regular engagement with cybersecurity matters during board meetings, where cyber risks are discussed with the same gravity as financial and operational risks. When leaders participate in cyber incident simulations and openly discuss security challenges, they send a powerful message about the organisation's commitment to cybersecurity.

Executive accountability forms another crucial pillar of this cultural transformation. By designating clear ownership of cyber risks at the executive level and incorporating cybersecurity metrics into performance evaluations, organisations create a direct link between leadership actions and security outcomes. The Chief Information Security Officer should have clear reporting lines to the board, ensuring that security considerations are represented at the highest levels of decision-making.

Embedding Security in organisational DNA

A positive cybersecurity culture flourishes within a well-structured organisational framework. Rather than treating security as a separate function, successful organisations weave it into the fabric of their operations. This integration begins with clear role definitions – every position within the organisation should understand its specific responsibilities in maintaining security. Security champions embedded within business units serve as local advocates and advisors, creating a network of security-conscious leaders throughout the organisation.

The policy framework supporting this structure must strike a delicate balance between comprehensiveness and accessibility. Effective security policies connect directly to business objectives, providing practical guidance for common scenarios while clearly articulating the organisation's security expectations. These policies should evolve through regular review and updates, ensuring they remain relevant to current threats and business practices.

Nurturing Security Awareness and Expertise

Building security awareness requires more than annual compliance training. Successful organisations develop comprehensive programs that engage employees through various channels and methods. Interactive workshops allow staff to explore security concepts in practical contexts, while scenario planning exercises help teams understand how to apply security principles in real-world situations. By gamifying certain aspects of security awareness, organisations can make learning more engaging and memorable.

Communication plays a vital role in maintaining security awareness. Regular updates about emerging threats, shared lessons from incidents, and celebrations of security successes help maintain focus on cybersecurity throughout the year. organisations should leverage multiple communication channels to ensure their messages reach all employees effectively.

Risk Management in Practice

Effective cyber risk culture manifests in how organisations approach day-to-day operations. Security considerations should be embedded in every significant business decision, from project planning to change management. Risk assessments should become second nature, conducted regularly and thoroughly, with results feeding into a broader enterprise risk framework.

Measuring the effectiveness of these efforts requires thoughtful selection of metrics. Rather than focusing solely on technical indicators, organisations should develop measurements that reflect the human aspects of security – how employees identify and respond to threats, their willingness to report concerns, and their understanding of security principles.

Learning from Experience

A mature security culture embraces incidents as learning opportunities. When security events occur, the focus should extend beyond immediate response to understanding root causes and improving processes. Regular simulation exercises help teams practice their response capabilities while identifying areas for improvement. Cross-functional response teams ensure that all aspects of an incident are considered, from technical resolution to stakeholder communication.

Incentivising Security Excellence

organisations must align their reward systems with their security objectives. This goes beyond punitive measures for security breaches to include positive recognition for security improvements and innovations. Security considerations should factor into performance reviews at all levels, and career development paths should recognise cybersecurity expertise as a valuable skill set.

Managing External Relationships

A strong security culture extends to relationships with vendors and partners. organisations should clearly communicate security expectations to third parties

and maintain regular oversight of their compliance. Collaborative security initiatives and shared threat intelligence can strengthen these relationships while improving overall security posture.

Measuring Cultural Progress

Assessing security culture requires both quantitative and qualitative measures. Regular surveys can gauge employee attitudes toward security, while behavioral metrics provide insight into how well security practices are being adopted. These assessments should feed into a continuous improvement cycle, allowing organisations to refine their approach based on what works best in their specific context.

The Path Forward

Building a strong cybersecurity risk culture is a journey rather than a destination. It requires sustained commitment, regular reinforcement, and continuous adaptation to evolving threats. Success comes from making security relevant to everyone in the organisation, measuring progress meaningfully, and maintaining focus on long-term cultural change rather than short-term compliance.

organisations that succeed in building a strong security culture find that it becomes a competitive advantage, enabling them to operate with greater confidence in an increasingly threatening digital landscape. Their employees become active participants in security, creating a human firewall that complements technical controls and enhances overall organisational resilience.

Comprehensive Mitigation Strategies

Financial institutions must adopt a multi-layered approach to address these evolving threats:

Security Architecture Evolution: organisations need to implement zero-trust architectures that assume no implicit trust, even for internal systems and users. This involves continuous verification of every user, device, and transaction across all environments - cloud, on-premises, and hybrid.

Advanced Detection and Response: Implementation of AI-powered security operations centers (SOCs) that can process and analyse vast amounts of security data in real-time. These systems must be capable of detecting subtle indicators of compromise across complex financial systems while minimising false positives.

Resilient Infrastructure Design: Development of infrastructure that can maintain critical financial operations even during active cyber attacks. This includes implementing sophisticated failover systems, maintaining secure offline backups, and regularly testing business continuity procedures.

Enhanced Customer Protection Framework

To protect customers effectively, financial institutions should implement:

Intelligent Transaction Monitoring: Advanced systems that use behavioral analytics and machine learning to detect unusual patterns in customer transactions,

blocking potentially fraudulent activities in real-time.

Multi-Factor Authentication Evolution: Implementation of sophisticated authentication systems that go beyond traditional two-factor authentication, incorporating biometrics, behavioral analysis, and context-aware authentication policies.

Customer Education and Awareness: Development of comprehensive security awareness programs that help customers understand emerging threats and practice safe financial behaviors. This includes regular updates about new threat types and practical security measures customers can implement.

Regulatory Compliance and Reporting

Financial institutions must maintain strong relationships with regulatory bodies and establish:

Incident Response Protocols: Clear procedures for reporting security incidents to relevant regulatory authorities, including detailed documentation of breach impacts and remediation efforts.

Compliance Monitoring: Continuous monitoring systems to ensure adherence to evolving regulatory requirements around cybersecurity and data protection.

Future Outlook

As we progress through 2025, financial institutions must remain vigilant and adaptable. The threat landscape will continue to evolve, driven by technological advancement and changing attack methodologies. Success in this environment requires a commitment to continuous security improvement and adaptation to emerging threats.

Further Reading and Useful Resources:

These sources provide a mix of real-time alerts, detailed reports, and strategic insights tailored to corporate cybersecurity.

Cybersecurity and Infrastructure Security Agency (CISA)

- **Description**: A U.S. government agency providing alerts, best practices, and updates on cybersecurity threats and trends.
- **Website**: https://www.cisa.gov/

Krebs on Security

- **Description**: A leading cybersecurity blog by Brian Krebs, covering data breaches, malware, and corporate cybersecurity trends.
- **Website**: https://krebsonsecurity.com/

SANS Internet Storm Center (ISC)

- **Description**: A free, community-driven threat analysis platform offering incident data and trend reports.
- **Website**: https://isc.sans.edu/

Dark Reading

- **Description**: A trusted online community for cybersecurity professionals with news, analysis, and insights.
- **Website**: https://www.darkreading.com/

BleepingComputer

- **Description**: A comprehensive resource for the latest in cybersecurity news, vulnerabilities, and tools.
- **Website**: https://www.bleepingcomputer.com/

The Hacker News

- **Description**: A popular cybersecurity news platform covering the latest threats, incidents, and corporate defenses.
- **Website**: https://thehackernews.com/

Threatpost

- **Description**: A trusted source for breaking cybersecurity news, insights, and vulnerability updates.
- **Website**: https://threatpost.com/

National Institute of Standards and Technology (NIST) Cybersecurity Framework

- **Description**: Provides standards, guidelines, and best practices for managing cybersecurity risk.
- **Website**: https://www.nist.gov/cyberframework

CSO Online

- **Description**: Provides security and risk management insights for corporate professionals.
- **Website**: https://www.csoonline.com/

SecurityWeek

- **Description**: Focused on IT and business security news, trends, and analysis.
- **Website**: https://www.securityweek.com/

ISACA Journal and Insights

- **Description**: Offers resources and thought leadership for IT governance, cybersecurity, and risk management professionals.
- **Website**: https://www.isaca.org/resources

AI use

An AI tool was utilised in the drafting process for this guide.