TOP 6 THREATS FACING FINANCIAL INSTITUTIONS IN 2025

Physical. Cyber. People.

In the financial sector, security is no longer just about defending against attacks it's about being proactive and resilient and actively looking for indicators of compromise around the clock, whilst staying compliant with regulation.

Cybercriminals choose their targets based on two key factors: maximum impact and maximum profit. Financial institutions are perfect candidates, holding vast amounts of valuable data and undergoing rapid digital transformation, which opens new doors for cyberattacks. This relentless pursuit of valuable data by criminals leads to a critical issue: the integrity of the data itself.

Data integrity is especially concerning when unauthorized alterations whether malicious or accidental affect financial or sensitive information, such as bank details.

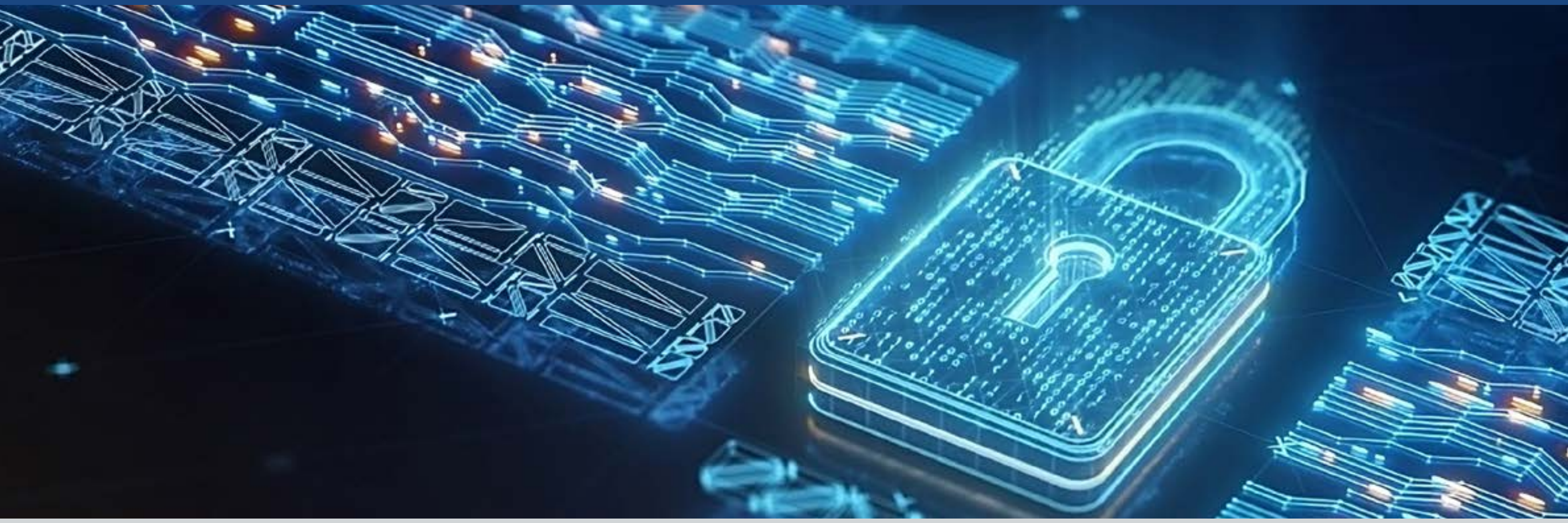
These compromises pose severe risks to financial stability and regulatory compliance. As cybercriminals increasingly target data manipulation, ensuring its accuracy and authenticity has become a top priority. Without strong data integrity measures, financial institutions risk operational disruptions, reputational damage, and diminished trust.

This growing vulnerability is having significant financial consequences for the industry. IBM reports that the average cost of a breach in the financial sector is $6.08 million.

To address these challenges, regulators like the Financial Conduct Authority (FCA) and the Bank of England have put strict measures in place. Tools such as CBEST, STAR-FS, and CQUEST help financial organisations identify weaknesses and strengthen their defences. Across Europe, frameworks like the Digital Operational Resilience Act (DORA) and the NIS2 Directive have further mandated robust standards for managing ICT risks and ensuring business continuity during disruptions.

John Edwards, the UK Information Commissioner, highlights a crucial point:

"The biggest cyber risk businesses face is not from hackers outside of their company, but from complacency within their company. If your business doesn't regularly monitor for suspicious activity, fails to act on warnings, neglects software updates, or doesn't train staff, you can expect significant fines."



Where to Focus - Understanding the Key Threats

While the regulatory requirements facing financial institutions are stringent, deciding where to focus efforts can be challenging. To help address this, the Bank of England's 2024 Systemic Risk Survey identifies the key areas of concern for the financial sector. The results echo previous years, with geopolitical risks (85%), economic risks (85%), and cyber threats (70%) topping the list, while climate risks (36%) are also noted. These findings underscore the interconnected nature of today's risks, with geopolitical and cyber threats often overlapping, amplifying their impact.

The sheer volume of threats identified, however, can make it difficult to prioritise appropriate steps and technical controls. Rankings of risks often vary, and such lists can be confusing, leaving organisations unsure of where to direct what Toro finds, is typically limited resources.

Adding to the complexity is the increasing convergence of security risks. Modern attackers often combine cyberattacks with physical breaches or insider threats, creating what's known as "converged threats" taking the path of least resistance. For example:

- **People –** Attackers gather intelligence on employees via social media or other public platforms, and even apply for your vacancies!
- **Cyber Security –** This intelligence is used to launch phishing, vishing and smishing attacks, gaining access to internal systems and deploying malware or exfiltrating your data.
- **Physical Security –**The attackers may exploit weak physical security measures, such as bribing staff or bypassing access controls, to steal data, hardware or to plant malware directly, or to gain intelligence that enables a more significant cyber-attack.

This overlap makes it clear that financial institutions need integrated holistic next-generation defence strategies. To help financial organisations navigate the vast amount of information, we've highlighted the top six key threats facing the sector in 2025 and provided actionable steps to address them.

Phishing and Social Engineering

Phishing - tricking people into revealing sensitive information remains a major threat. In 2023, 27.3% of global phishing attacks targeted financial institutions, underscoring the sector's vulnerability.

Mitigation Strategies:

- **Digital Footprint Reviews -** Regularly review your organisation's digital footprint to identify exposed employee details or breached credentials that attackers might exploit.
- **Resilience Testing -** Conduct simulated phishing tests, including "Quishing" (QR code phishing) and Vishing (voice phishing), to measure employee awareness and response. Attackers will try to impersonate you verbally as well as digitally!
- **Cyber Hygiene Training -** Provide regular training to employees, equipping them with the skills & confidence to recognise and report suspicious activity without fear of retribution.
- **Technical Controls -** Choose controls that offer both conditional access and heuristic and behavioural analysis in their approach to stopping phishing attacks, that can determine the difference between benign and malicious actions and stop any inappropriate processes from executing. Antivirus is no longer suffice, and Toro recommends a defence-in-depth strategy is layered to protect sensitive data and systems.

Cloud Security Issues

As financial institutions continue to embrace digital transformation, the shift to cloud environments introduces new complexities and vulnerabilities that must be carefully managed. The expansion of digital footprints, coupled with remote and hybrid working, significantly broadens the potential attack surface making organisations more susceptible to cyber threats. Cloud breaches can be catastrophic because they provide cybercriminals with direct access to sensitive data and systems, potentially allowing them to operate undetected for extended periods of time.

Mitigation Strategies

- **Asset Management –** knowing what you have is the first step to securing it. Consider IT sprawl and shadow IT.
- **Penetration Testing -** Simulate frequent real-world attacks to identify vulnerabilities in applications, networks, and systems.
- **Endpoint Security -** Secure devices used for remote work through Next Generation solutions like Managed Detection and Response (MDR), which offers 24x7x365 human-led monitoring and incident response capabilities that proactively seek out Indicators of Compromise (IoC) and can integrate with your cloud architecture.
- **Cyber Essentials Certification -** Adopt government-backed standards that address critical security measures, from firewalls to software patching.

- **Third Party Risk Assessment -** To manage third-party risks effectively, organisations should carefully evaluate the cloud providers' security policies, practices, and past track records. The Shared Responsibility Model outlines the division of security duties between the cloud service provider (CSP) and the financial institution. Institutions must understand which aspects of security the CSP is responsible for and which they are accountable for. Service Level Agreements (SLAs) should be reviewed to ensure that the CSP is providing the necessary guarantees for uptime, data protection, and incident response.

- **Data Loss Prevention (DLP) -** DLP strategies protect sensitive information from unauthorized access or leakage. This involves enforcing policies that ensure the integrity of data, preventing unauthorized alterations, and ensuring non-repudiation. DLP tools monitor and control data movement across cloud environments, detecting any attempt to send or store sensitive information in an insecure manner.

- **Secure Access Service Edge (SASE) –** Using the latest technologies such as SASE, you can significantly reduce your attack surface by removing cloud infrastructure from being public internet facing, to being secure private network facing. Couple this with Cloud Access Security Broker (CASB) – typically part of SASE – and you can restrict access using Zero Trust Network Access principles to secure your cloud infrastructure through conditional access at the Internetwork level. This new and emerging technology protects your cloud infrastructure when SASE capabilities are successfully implemented, removing exposure to the likes of AWS, Azure, and any private cloud infrastructure you host.

Supply Chain Risks

A single weak link in the supply chain can compromise an entire organisation. Attackers are increasingly seeking to exploit third-party partners with less robust security to gain access to financial institutions.

Mitigation Strategies

- **Due Diligence -** Investigate the operational history, financial stability, and compliance records of suppliers before entering into agreements.

- **Third-Party Risk Assessments -** Evaluate the security posture of all suppliers and partners, with a view to enforce strict policies on data sharing that at least match the level of security stated in your own policies and procedures as a minimum baseline.

- **Zero Trust Frameworks -** Implement a “never trust, always verify” model to ensure continuous authentication and limited access, even for trusted parties, with Just Enough Administration (JEA) to be able to perform the functions they need to, and no more. The principle of least privilege will minimise impact and disruption in the event of an incident.

- **Defence in Depth Strategy –** attackers will be more and more persistent and the threat landscape is prolific. Layered security makes it less appealing and more difficult to breach your systems. Applying technical controls in a layered fashion builds your defences in a way that is most challenging to overcome. If your defences are stronger than your competitors, you are less susceptible to being targeted.

Advanced Persistent Threats (APT)

Advanced Persistent Threats (APTs) are long term, sophisticated cyber-attacks, usually carried out by skilled, well-funded groups like nation-state threat actors. These attacks aim to infiltrate financial institutions' networks and remain undetected for extended periods, stealing sensitive data or causing disruption. APTs are particularly dangerous for financial institutions because of the high-value data they manage, such as personal, financial, and transaction information.

APTs often begin through vulnerabilities, phishing, or weak security, with attackers establishing a foothold inside the network. Once in, they can move laterally, gather information, pivot, and execute their goals whilst evading detection. The impact on financial institutions can be severe, with data breaches, financial theft, and reputational damage. APTs can also instigate other attacks, such as DDoS attacks, to further divert attention or create chaos while the attackers remain inside your networks, undetected.

A DDoS (Distributed Denial-of-Service) attack is a type of cyberattack where multiple compromised systems flood a target system, such as a website, an application, or server, with excessive traffic. This overwhelms the system, causing it to slow down or go offline entirely, disrupting services and diverting attention away from other ongoing attacks, like APTs. DDoS attacks are a popular cyber threat against financial services because their attack surface is diverse, comprising banking IT infrastructures, customer accounts, payment portals, and other critical systems that typically need to be public facing.

Mitigation Strategies

- **Traffic Monitoring -** Monitor all network traffic, including internal and external traffic, to detect irregularities.

- **Access Control and Privilege Management -** Implement strict access controls using multi-factor authentication (MFA) and least privilege principles. Regularly review user permissions and ensure sensitive systems require additional verification steps to prevent lateral movement within the network.

- **Regular Security Updates and Patching -** Ensure all systems, applications, and devices are updated with the latest security patches. Conduct regular vulnerability scans to identify and address weaknesses before they can be exploited by attackers.

- **Reducing The Attack Surface –** By reducing the attack surface, you remove risk of an incident occurring. This consideration needs balance, as to not impact business as usual activities, but is a good way to limit the damage that can be caused.

- **Build with Resilience -** Systems should be designed to be secure, with resilience and redundancy at the forefront of your architecture design.

- **Implement DDoS Protective Solutions –** organisations can seek to evade DDoS attacks through the use of services and technologies that seek to strip out DDoS attacks at the WAN internet layer, to avoid disruption and down time. For services that are revenue critical, DDoS prevention is imperative and should be a commodity consideration.

Insider Threat

Insider threats have escalated as a critical security concern for organisations, with a staggering 71% of companies experiencing between 21 and 40 insider incidents annually, a 67% increase from 2022.[1] The financial impact of these incidents is severe, now averaging $11.5 million annually. Despite the growing awareness, fewer than 30% of organisations believe they have the right tools to combat insider threats effectively.

Mitigation Strategies

- **Pre-screening and Vetting -** Implement thorough background checks and online activity reviews for employees with privileged access.

- **Digital Footprint Monitoring -** Regularly monitor employees' digital activities, especially senior staff, to prevent attackers from exploiting publicly available information. A review of the Dark Web is an important consideration, as attackers may try to breach employees at a personal level in order to attack organisations through bribery and blackmail.

- **Continuous Risk Assessments -** Conduct ongoing evaluations of staff behaviour and access to sensitive data to identify potential insider threats early.

- **Zero Trust Frameworks -** Implement a "never trust, always verify" model to ensure continuous authentication and limited access, even for trusted parties, with Just Enough Administration (JEA) to be able to perform the functions they need to, and no more. The principle of least privilege will minimise impact and disruption in the event of an incident.

- **Joiners, Movers, and Leavers –** Ensure you have solid processes in place for Joiners, Movers, and Leavers to provide the least privileges needed for joiners to conduct their role, and that any and all permissions are revoked as appropriate when employees move departments or leave the business, to swiftly reduce the attack surface at the identity level within your business.

[1] https://www.aon.com/en/insights/articles/mitigating-insider-threats-your-worst-cyber-threats-could-be-coming-from-inside

Ransomware

Ransomware remains a severe and escalating threat to financial institutions, with cybercriminals using malware not only to encrypt data and demand ransom for its release but to exfiltrate data and sell the data to other cyber criminals. Financial organisations are particularly vulnerable due to the high value of the sensitive data they hold. In addition to disrupting operations and causing data loss, ransomware can lead to significant reputational damage and regulatory consequences.

Mitigation Strategies

- **Regular Backups -** Ensure data is regularly backed up to a secure location, minimising the impact of a potential ransomware attack by making it easier to restore data without paying the ransom.

- **Incident Response Plan -** Develop and continually test a robust incident response plan that includes detailed steps for handling ransomware, communication protocols, and reporting requirements to ensure timely and effective action in case of an attack.

- **Continuous Monitoring -** Implement continuous network monitoring and detection tools to identify ransomware activity early.

- **Employee Awareness & Training -** Regularly train staff to recognise phishing attempts and other common attack vectors used in ransomware campaigns. Empowering employees with knowledge is crucial in preventing initial breaches, turn your employees into your greatest strength not your greatest weakness.

- **Due Diligence -** As part of your due diligence make sure you are checking for data on the dark web re your organisation.

- Using **Next Generation technical controls** that monitor for remote execution ransomware and local ransomware attacks, that use heuristic analysis to determine a ransomware attack is underway, and enables you to roll back any ciphered data.

- Using Data Loss Prevention (DLP) and Application Control technologies to prevent sensitive data leaving the business, and blocking access to file sharing applications including FTP, SSH, and less secure variants such as Telnet can help you keep your confidential data confidential!

Moving Forward

The financial sector is at a critical juncture. As threat actors become more sophisticated, organisations must evolve their defences to stay one step ahead. This means embracing comprehensive strategies that integrate cyber, physical, and insider security measures.

By prioritising training, investing in advanced tools, and adopting methodologies such as Zero Trust Network Access, financial organisations can mitigate risks, protect their data, and maintain the trust of their customers.

While the road ahead is challenging, taking proactive steps now will strengthen resilience and ensure long-term stability in a rapidly changing threat landscape.

Toro was founded on creating the UK's first Red Team penetration test - and then attacking hundreds of clients by hacking their systems, influencing / social engineering staff and breaking into their offices - replicating blended threats from organised crime and hostile nations.

The gaps we found were the same across most businesses. The defenders were still siloed and not collaborating to protect against blended threats.

That's where we're different.

We take an attacker's mindset to defend our clients.

We ATTACK our clients, DEFEND them, MANAGE their IT, OPTIMISE their cyber security posture and physical security, and RESPOND when they are attacked.

Most clients just want a single trusted security partner that can manage all their security needs - so the business can grow and succeed, Toro is this partner.

🌐 **www.torosolutions.co.uk**
✉ **info@torosolutions.co.uk**
☎ **0208 132 9267**

Physical. Cyber. People.