AI's Impact on the Evolving Cyber Threat Landscape for Capital Markets

November 2025

Foreword

AFME and PwC UK convened over the summer of 2025 a series of roundtables with senior banking executives representing wholesale capital markets, to explore emerging AI-related risks, the measures banks are implementing, and the role of regulation in enabling AI adoption in a secure way. The following paper, co-authored by PwC UK and AFME, summarises the key insights from these discussions, with thanks to Clifford Chance for their assistance on the regulatory dimension.

Executive Summary

AI (Artificial Intelligence) technologies are becoming increasingly embedded within financial services. This is altering the cyber threat landscape, with the technology harnessed by hackers into new forms of attack, for example advanced phishing and deep fakes. To explore these shifts in further depth, AFME and PwC convened a series of roundtables over the summer of 2025. These discussions highlighted that:

- The resulting impact is primarily one of scale and pace, where the underlying attack vectors and drivers remain the same, but the volume and sophistication of attacks are now at a much-heightened scale. In tandem, this means the margins within which a firm must respond are significantly intensified.
- Financial entities are already responding to these external shifts in cybercrime, through a range of essential mitigations such as inoculating users through isolated browsers and sandboxing of inboxes, and by working with vendors and suppliers on enhanced security measures.
- Internally, firms are also putting in place enhanced governance supported by automated controls to ensure that the deployment of AI happens safely and that employees are appropriately trained and skilled.
- Crucially, while misguided AI deployment internally can introduce new risks, these technologies can also serve to protect organisations and secure them from external attacks.
- When putting in place these strategies, firms are mindful of the increasing regulatory and supervisory expectations in this space. These can at times be conflicting and overlapping from the perspective of a multi-national bank, and AFME will continue to stress to regulators how compliance is best demonstrated from an outcomes-based approach.
- AFME has additionally noted the role of cyber security agencies and joint public-private forums. The guidance produced by these bodies to date can provide a baseline for firms' incident response and management, and it is worth echoing how these agencies and our members have both highlighted that AI can itself be part of the solution.

AI and the Evolving Threat Landscape for Capital Markets

Artificial Intelligence (AI) is no longer a novelty in financial services—it is increasingly embedded, albeit outside core business services for now, and has unleashed new opportunities for banks, their clients and stakeholders. On the flip-side, AI also enables cyber attackers; making their attacks harder to detect, faster, better and more intense. The motivations and methods behind AI powered attacks remain familiar, but the speed and volume at which they occur have intensified exponentially. Additionally, whilst AI is helping to empower non-IT employees within banks with advanced programming and data analysis capabilities, this democratisation introduces new risks.

Banks have repeatedly shown they can rapidly adapt to such seismic shifts. In the past decade they have enabled secure adoption of Cloud, Crypto, DLT (distributed ledger technology), BYOD (bring your own device), big data, remote working and APIs (applications programming interfaces). Banks have matured, layered defence strategies and are adept at tuning these in the face of new threats and new technologies. Whilst the past decade was not entirely without incident, the adoption and enablement of all these technologies has been relatively uneventful.

With the right focus and approach, it is expected banks will achieve the same successful and secure deployment of AI, to the benefit of their clients and stakeholders.

How and where are Capital Markets seeing these AI risks appear, both externally and internally? And what are they doing to tackle such risks?

AI use by bad actors has not altered the underlying behaviours or motivations of cyber attacks, but their likelihood (frequency, velocity, strength and breadth) has increased exponentially during the period of global AI adoption. Banks are having to harden their defences and automate their controls in new ways. Driven by this increased likelihood of cyber attack these mitigations have emerged as essential practice.

Table 1: External AI Threats to Banks

Threat	*Summary*	*Essential Mitigation*
Smarter Phishing Attacks	AI makes phishing more convincing, especially in unfamiliar languages.	Use isolated browsers, sandboxed inboxes, and increase employee awareness.
Patch Management Pressure	Weaponisation of new vulnerabilities occurs in hours, not months.	Re-balancing speed with oversight— Cyber teams validate patches while security teams automate patching.
Supply Chain Weak Spots	Vendors often lack strong cyber defenses, making them easier targets than banks.	Strengthen third-party risk management, vendor oversight, engagement with vendors and intelligence sharing.
Shape-Shifting Threats	AI can evolve attack methods to complicate detection.	Faster real-time threat intelligence, and heuristic analysis. Respond more on unusual patterns, and not “known bad” signature-based detections.
Credential Manipulation	AI can trick staff into following fake but plausible internal processes.	Reinforce internal controls and train staff to question unusual requests.
Deepfake Deception	AI-generated voices and videos can impersonate trusted individuals.	Enforce multi-factor authentication and verify sensitive requests through multiple channels.
Testing Gaps in AI Defense	AI threats are not yet fully integrated into cyber testing frameworks.	Embed AI scenarios into cyber tests; ongoing testing of AI security.
Cybercrime at Scale	AI is driving exponential growth in cyber attacks for firms to respond to.	Automate defence measures to accelerate response without human involvement.

In parallel to these external risks by bad actors, corporate adoption of AI introduces a multitude of new internal risks. This is why banks who are deploying AI are introducing new AI security governance frameworks and controls to ensure safe, secure and compliant AI.

Table 2: Threats introduced by the internal deployment of AI

Threat	*Summary*	*Essential Mitigation*
Leaky Internal LLMs (large language models)	AI tools may divulge outdated or sensitive data.	Auto classify data; limit data input; use security AI to monitor prompts and outputs.
Employee-Led AI Use	Staff empowered with AI can create insecure or risky deployments.	Enforce internal guidelines and training for AI use; implement continuous testing against model drift; limit AI access and identify unusual requests.
New Targets: MCP Servers (Model Context Protocols)	AI infrastructure like MCP servers opens new attack surfaces.	Harden legacy systems (VPNs), by moving to strong authentication / zero trust; harden and monitor AI infrastructure closely.
Agentic AI Risks	Autonomous AIs could misinterpret tasks or bypass controls.	Enforce strict role-based access; use non-human identities; and audit AI outputs with oversight AIs and humans.
Instructions in data	Embedding malicious instructions in data inputs (pictures, videos) can bypass detection.	Screen data inputs for hidden instructions; only process instructions; monitor threat intelligence for evolving exploits.

How is the regulatory environment shaping the AI evolution?

There are multiple current regulations relevant to AI usage within Capital Markets (e.g. AI Act, DORA and NIS2), which collectively address senior ownership and governance, incident reporting and risk management. At times this results in a complex and mismatched global patchwork of obligations for firms which could trigger another wave of contractual clause amendments by banks, at a time when firms are just wrapping up the wave of DORA remediations. Yet it is crucial that firms are aware of those regulatory obligations which directly impact the management of AI related risk.

Table 3: Regulatory obligations facing firms relating to AI risk (*non-exhaustive)

Regulatory Obligation	*Implementation Challenge*	*Essential Mitigation*
Governance & Accountability	Accountability gaps should not emerge despite the complex regulatory landscape	Adopt a holistic risk-based governance model to best satisfy complex regulatory landscape.
Data Protection	AI providers should not be allowed to retain sensitive data for training.	Update contracts with current AI providers to ensure that sensitive data is ringfenced or carefully permitted within sandbox environments.
Incident and vulnerability reporting	The EU AI Act adds even more regulatory reporting requirements to firms.	Integrate the definition of High Risk AI to corporate inventories and further adapt incident reporting procedures to include the new reporting requirements.
Deployer vs Provider	The AI Act's differing requirements for AI Providers versus AI Deployers are likely to cause confusion as firms adopt and modify the use of third-party AI products, which may shift their role from a Deployer to a Provider.	Adopt continuous governance over AI systems; define and monitor for events that may change the firm's role from Deployer to Provider.

Conclusion

Just like other “emerging technologies” widely adopted over the past decade, AI presents huge potential benefits for banks, clients and their stakeholders. In the wrong hands, AI can present a substantial security risk, but unlike other emerging technologies, AI can also be the solution to many of the security problems that it introduces, helping banks to become faster, and more targeted in security, to look beyond signatures to patterns, and to propose improvements to data or identity management controls.

As the technology matures, AI s dual role as both risk and remedy will define the next chapter in financial cybersecurity, and during this period it is important regulators support the timely and innovative application of essential mitigations that keep Banks secure, and push for harmonised regulatory frameworks to help unleash the broader benefits.

Contacts

Marcus Corry
Director
AFME
marcus.corry@afme.eu

Fiona Willis
Director
AFME
fiona.willis@afme.eu

Chris Girling
Partner, Cyber Security and Resilience
PwC Switzerland
chris.girling@pwc.ch

Christian Arndt
Director, Cyber Security and Resilience
PwC UK
christian.arndt@pwc.com

afme/

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

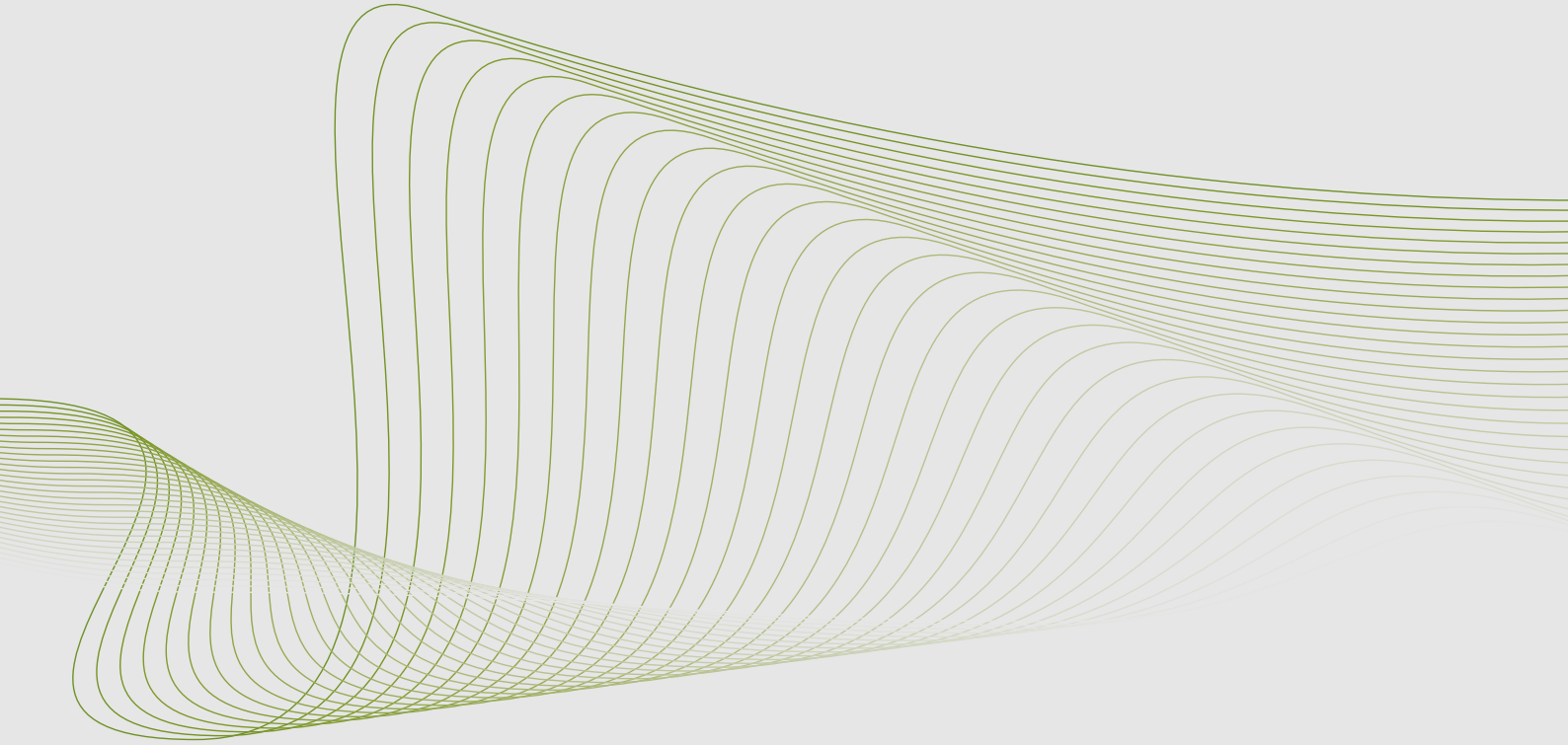
Expertise
deep policy and technical skills

Strong relationships
with European and global policymakers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)



London Office
Level 10
20 Churchill Place
London E14 5HJ
United Kingdom
+44 (0)20 3828 2700

Press enquiries
Rebecca Hansford
Head of Communications
and Marketing
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 883 5540

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Frankfurt Office
Große Gallusstraße 16-18
60312 Frankfurt am Main
Germany
+49 (0)69 710 456 660

AFME is registered on the
EU Transparency Register,
registration number
65110063986-76

www.afme.eu