Cyber-crime continues to test the post-trade industry

Geopolitical risk may be the biggest threat facing financial institutions today, but cyber-crime is not far behind in second place. In 2010, cyber-attacks shaved around $100 billion off the global economy[1] – fast-forward 15 years, those costs have risen by more than 100-fold to $10.5 trillion, and they are expected to shoot up even further – potentially hitting $15.63 trillion by 2029.[2]

Responsible for safekeeping trillions of dollars in cash and securities, custodians and central securities depositories (CSDs) are prime targets for cyber-criminals. **Matthew Bax**, Head of Client Service and Sales for Citi Investor Services recently sat down with **Guillaume Eliet**, Group Chief Risk Officer at Euroclear, **Alexander MacLean**, EMEA Head of Cyber for Citi, and **Sille Stener**, Chief Technology Officer at Euronext Securities, to talk about cyber-crime and what the industry is doing to protect itself.

Cyber-crime keeps the risk teams up at night

Cyber-crime is not a risk that financial institutions take lightly – in fact, 69% of firms indicated on the Depository Trust & Clearing Corporation's (DTCC) annual Systemic Risk Barometer survey that cyber-crime was the most serious threat they face, superseded only by geopolitical risk at 84%.[3]

The consequences of being hacked can be devastating – "The risks facing our organisations from cyber-attacks are much more than just financial – it is also reputational and systemic. The reality is that when a financial institution is hit by a cyber-attack – all other risks, such as credit and operational risk – are exacerbated as well," said **Bax**.

Cyber-attacks come in many different shapes and sizes.

"DDOS [Distributed Denial of Service] attacks are when bad actors disrupt a company's website by overwhelming its infrastructure with web traffic, causing the website to crash – this often means customers and employees cannot access the website. In Europe, there was a recent DDOS attack on a leading third-party payments app, which led to users suffering from widespread disruption. A DDOS attack is often deployed by criminals to test the strength of a company's cyber-security," noted **MacLean**.

Contributors

Matthew Bax
Head of Client Service and Sales for Investor Services, Citi

Guillaume Eliet
Group Chief Risk Officer, Euroclear

Alexander MacLean
EMEA Head of Cyber, Citi

Sille Stener
Chief Technology Officer, Euronext Securities

[1] The Guardian – October 30, 2013 – Online fraud costs global economy many times more than $100 billion
[2] Viking Cloud – July 15, 2025 – 193 cyber-security stats and facts for 2025
[3] DTCC – December 4, 2024 – Geopolitical and Cyber Risk remain top threats to the financial services sector in 2025

Maclean added: "If cyber weaknesses are found in a DDOS, then the criminals may target the company with an even more sophisticated attack, potentially one that leverages ransomware – a type of malware that prevents people from accessing company devices and data through encryption."

For most cyber-criminals, their primary motivation for doing what they do is financial. This is because in exchange for gaining access to their encrypted data or having a DDOS attack called off, some – but not all – companies may be tempted into paying the cyber-criminals a ransom. According to a study by Sophos, a cyber-security company, nearly 50% of companies who suffered a hack paid a ransom to retrieve their data.[4] The sums involved are non-trivial – ransom payments typically average around $5 million for companies whose revenues exceed $1 billion.[5]

Cyber-crime is a lucrative business, and one that has become increasingly institutionalised, according to **Stener**. "Today's crop of cyber-criminal networks are professional businesses, and some of them are sponsored by governments. These networks may even have dedicated service desks where companies who have been hacked can negotiate with their attackers – these crimes are no longer just being perpetrated by lone individuals in basements," she said.

Regulators take a stand

As cyber-crime-related losses continue to mount at financial institutions, regulators and policymakers globally are taking decisive action.

In the US, the Securities and Exchange Commission (SEC) adopted its 'Cyber-Security Risk Management Strategy, Governance and Incident Disclosure Rule' in 2023, requiring public companies – including banks – to disclose material cyber incidents within four business days of them happening. Similarly, in the UK, incident reporting processes are being toughened up for companies under the recently introduced Cyber-Security and Resilience bill.

According to **MacLean**, the EU has also been busy developing cyber-security regulations – including the Network and Information Systems Directive 2 (NIS2), which aims to enhance the cyber-resilience of essential services and digital infrastructures, and the Digital Operational Resilience Act (DORA), which establishes a harmonised EU-wide framework for ICT risk management, incident reporting, testing, information sharing, and third-party risk management across financial firms.

"The EU is pushing through with its Cyber Resilience Act (CRA) too. Amongst other things, the CRA requires that digital products need to be cyber-ready and safe from a cyber-security perspective. One of the areas of contention, however, is that the CRA requires firms to disclose where their digital products may have potential cyber vulnerabilities, a policy which if enacted, might invite scrutiny from bad actors," continued **MacLean**.

The penalties – both financial and reputational – of falling foul of these rules should not be underestimated. In the case of DORA, for example, the European Supervisory Authorities (ESA) have the power to fine companies up to 2% of their annual turnover for non-compliance.[6] Firms therefore have little choice other than to follow the rules to the letter.

Banks jump into action

With cyber-attacks becoming increasingly sophisticated and regulators taking a growing interest in financial institutions' cyber-hygiene practices, complacency is not an option. Cultural attitudes towards cyber-security are set by the top – if the C-suite prioritises cyber-security, then so too will the rest of the organisation.

"In terms of cyber risk mitigation, we are constantly monitoring the cyber risk levels facing our business. Our approach to cyber risk is constantly evolving – we review our cyber risk practices to adapt to the evolving threat, and this is a process that involves the board and executive committee [Exco]," said **Eliet**.

Equally important, continued **Eliet**, is that financial institutions share information with each other on cyber-security matters, and have open communication channels with law enforcement.

Together with having robust cyber risk assessment frameworks and detection tools, employees also need to be educated about the importance of taking cyber-security seriously and subjected to regular testing, e.g. simulated phishing exercises, so that best practices are upheld.

Other preventative measures include having thorough oversight of third-party vendors and potentially even fourth party vendors – after all a financial institution is only as strong as its weakest link. This comes as 96% of financial institutions reported they had been impacted by a cyber breach at a third party – a significant increase from 2024, when that figure stood at 78%.[7] "We are spending more time with our vendors and conducting enhanced testing," noted **Stener**.

Although financial institutions are being incredibly proactive on cyber-security – the industry's ability to accurately forecast cyber-attacks – and their impact – at least relative to other market and operational risks – is still in its infancy.

"Banks and intermediaries have a massive infrastructure to deal with credit risk, which costs the industry about $400 billion in losses each year. But when you think about credit loss, it is predictable, cyclical and capital backed – it is embedded into our risk frameworks. In contrast, cyber is not predictable and not fully capital based," said **Bax**.

While prevention and detection measures are integral cyber-defences, no financial institution – irrespective of how much capex it earmarks for cyber-security – will ever be fully shielded from hacks or breaches. Having in-built recovery and resilience procedures is all but essential if firms are to ensure business continuity following a successful attack.

At the same time, it is equally vital organisations test their recovery plans on a regular basis across a number of different black swan scenarios. "In terms of spending, it is important that organizations challenge how much they spend on cyber prevention measures and detection systems versus recovery. The biggest challenge facing any organisation is their ability to recover swiftly from a cyber-attack," said **Eliet**.

[4] Sophos – June 24, 2025 – Nearly half of companies opt to pay the ransom, Sophos report finds
[5] Sophos – June 24, 2025 – Nearly half of companies opt to pay the ransom, Sophos report finds
[6] Grant Thornton – August 6, 2024 – Digital Operational Resilience Act (DORA): Regulation Summary
[7] Security Brief – June 10, 2025 – Third party cyber breaches surge 25% in Europe's top banks

New threats on the horizon

While disruptive technologies can unlock all sorts of productivity and efficiency gains, they also expose financial institutions to new – and often unknown – cyber-risks.

Take Artificial Intelligence (AI), for example.

Cyber-criminals are already using the technology to refine and enhance their social engineering techniques and manipulate video and audio content (e.g. voice cloning) for financial gain. There are growing reports of companies suffering losses due to employees wiring funds to fraudulent accounts, after having video calls with deep-fake versions of their CFOs or COOs.[8]

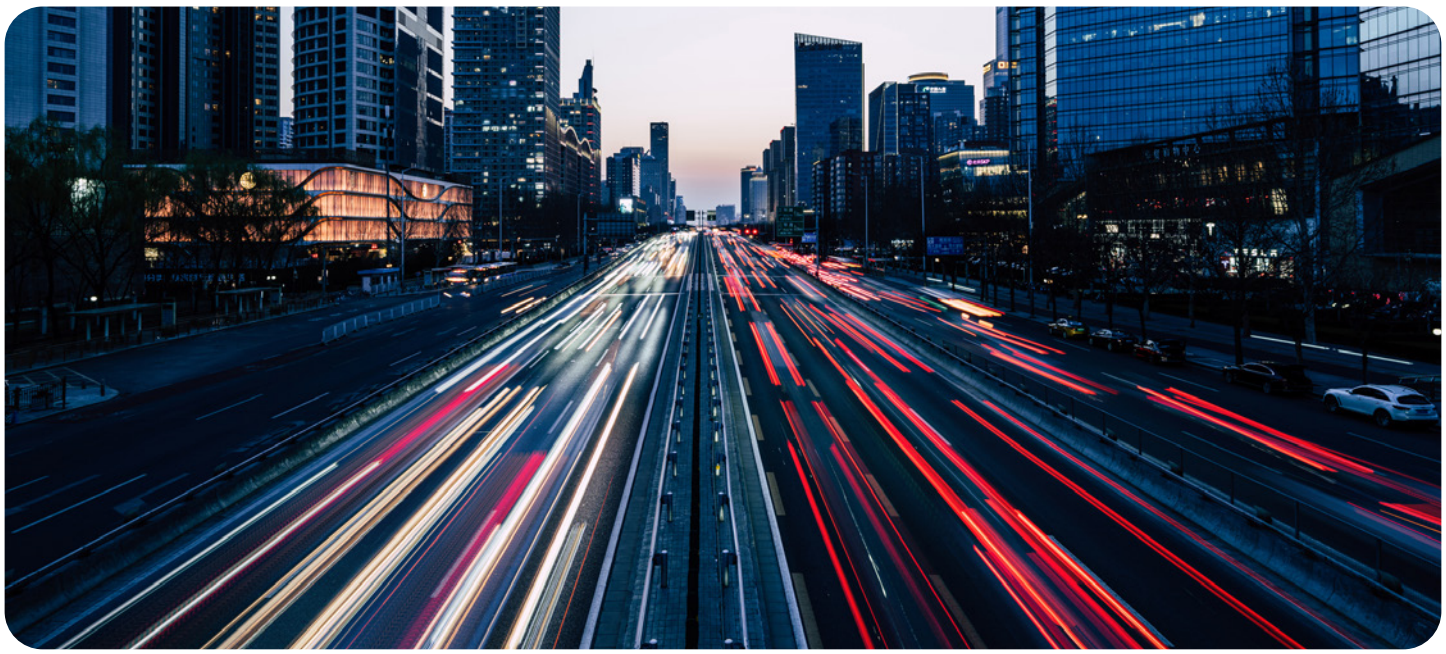
Longer-term, government agencies, including the UK's National Cyber Security Centre, have warned that AI enabled vulnerability research and exploit development could enable cyber-criminals to access systems through the discovery and exploitation of flaws in the underlying code or configuration.[9] Compounding matters even further is that as AI is so easily accessible, the barriers to carrying out disruptive cyber-attacks have also been lowered.

Other innovations, including quantum computing, a type of computer that harnesses quantum technology to solve complex problems, could also spark trouble for cyber defences.

"Quantum computing is not real yet, but we expect it to be real within the next seven to eight years. We are currently working towards encryption measures that will be able to stand up to quantum. While all the data we send across the Internet today is encrypted to today's standards, there are fears that people are scraping and holding onto this data, with the intention of leveraging quantum computers one day to decipher it," said **MacLean**.

As new technologies rapidly emerge, financial institutions need to build guardrails to ensure they fully understand the cyber-risks that come with them.

Cyber-threats are not going away – if anything, they are getting progressively worse. Financial institutions have little choice but to ensure that their prevention, detection and resilience protocols go beyond industry best practices. A failure to take cyber-crime seriously risks opening organisations up to serious financial, regulatory and – ultimately reputational – damage.



[8] Private Funds CFO – June 3, 2024 – Your Zoom call with your executive team? They were AI bots
[9] National Cyber Security Centre – May 7, 2025 – Impact of AI on cyber threat from now to 2027

25-93E9FACA 12/25