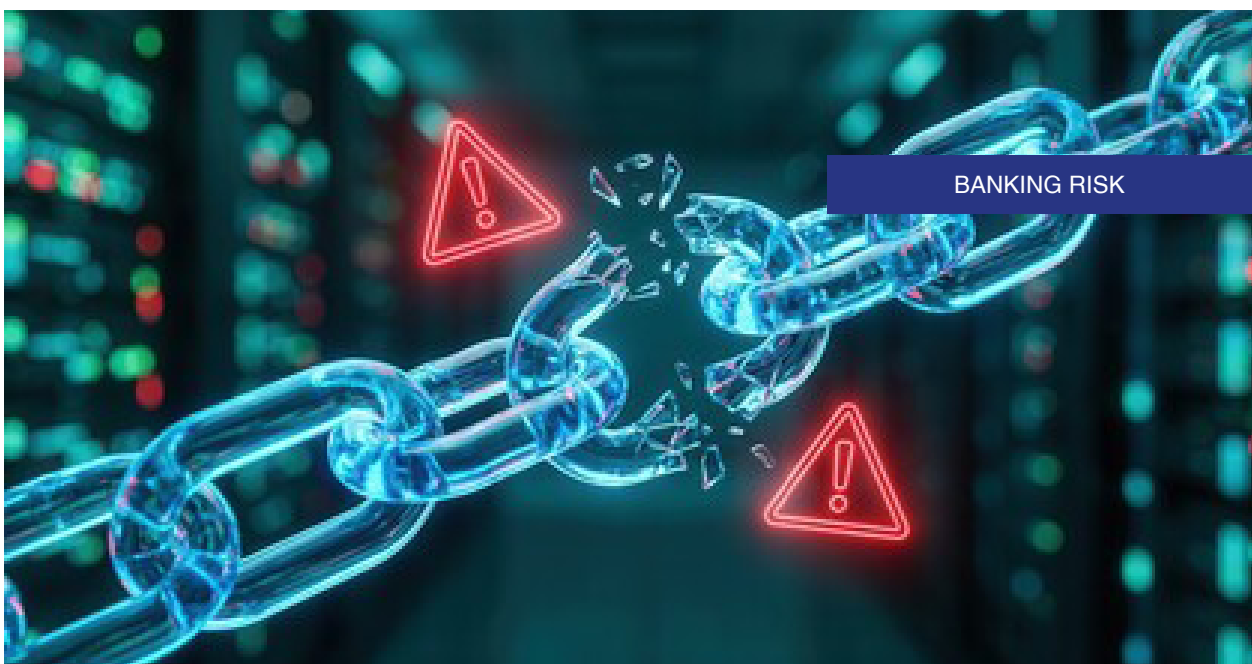




European banks and cyber risk: How AI is changing the equation

Cyber risk remains the top operational concern for European banks, cited by nearly three-quarters of institutions even as reported attack rates ease and realized losses continue to climb. Artificial intelligence now sits on both sides of this equation, sharpening banks' detection and response capabilities, while equipping adversaries with faster, more convincing tools of their own.

Pedro Cuadros-Solas and Nuria Suárez

Abstract: European banks absorb the majority of cyberattacks recorded across the region's financial system, accounting for 56.5% of incidents and making them the sector's principal target. Their exposure stems from managing extensive digital infrastructure and services, whose disruption is immediately visible and costly. The entry into force of DORA (Digital Operational Resilience Act) has tightened incident reporting, stress testing and oversight of external technology providers, formalizing obligations that

previously varied widely across institutions. Artificial intelligence is reshaping this landscape from the defensive side, enabling faster anomaly detection, alert triage and vulnerability remediation, as demonstrated by initiatives such as Anthropic's Project Glasswing. However, the same capabilities lower the barrier to sophisticated attacks, with 82.4% of banks identifying AI-enabled social engineering, deepfakes and credential theft as their foremost concern. Durable resilience will depend less on any single control than

on governance frameworks that treat AI simultaneously as a defensive asset and a source of concentrated, supplier-linked risk.

Introduction

This paper analyses the European banking sector's exposure to cyber risk, the implications for its operational resilience and the potential role of artificial intelligence (AI) in mitigating or amplifying this source of operational risk. Using EuRepoC and European Banking Authority (EBA) data, we show that the banks have been the victims of a substantial share of the cyberattacks sustained in the European financial sector and that cyber risk constitutes their biggest operational concern. Although the share of banks reporting recent attacks has fallen, the losses materialised as a result of those events have increased. AI has the potential to reinforce the detection of vulnerabilities and the defensive response but could also fuel faster, more automated and more sophisticated attacks.

Cyber risk, operational resilience and AI

Digitalisation is thoroughly transforming the banking business. A growing percentage of transactions are being carried out through digital channels. Payments are processed in real time, employees access applications and data from multiple environments and the banks depend on complex networks of technology service, market infrastructure and cloud platform suppliers. Admittedly, this transition is reducing costs, improving the customer experience and broadening the service offering. However, it is increasing the attack surface in parallel.

Cyber risk is no longer merely a technical issue: it has become a key source of operational risk. Incidents could prevent customers from accessing their accounts, disrupt payments, compromise confidential information, corrupt data or facilitate fraudulent transactions. Operational resilience, therefore, does not consist solely of preventing incidents. It implies identifying critical functions, anticipating adverse scenarios, mitigating the impact of a disruption and restoring service. Against this backdrop, the Digital Operational

Resilience Act (DORA), in force since 17 January 2025, tightens the management of ICT risk, notification of incidents, stress tests and control of external technology suppliers (European Union, 2022).

AI-based tools have the ability to enhance the detection of anomalies, analyse high volumes of alerts, identify vulnerabilities and accelerate the bank's response to incidents. However, those same capabilities can be used by threat actors. The EBA believes that the rapid development of frontier AI models could amplify operational and cybersecurity risks through the malicious use of AI-based tools.

The aim of this paper is to analyse the significance of cybersecurity risk for the European banks and its impact on their operational resilience. To do that, we first look at the banks' position as a target for cyberattacks aimed at the financial sector. We then examine the perception of operational risk and recent trends in the attacks suffered by the banks. Lastly, we analyse the double-edged role of AI as a defensive tool and potential threat amplifier.

The banking sector in the crosshairs of cybercriminals

Cybercriminals are particularly attracted to banks. The banks manage money, personal data and passwords; play a core role in payment systems; have ties with numerous customers, businesses, public authorities and suppliers; and provide services whose disruption is immediately apparent. A cyberattack can in one fell swoop generate a financial gain for the attacker, a high cost for the bank and significant reputational damage.

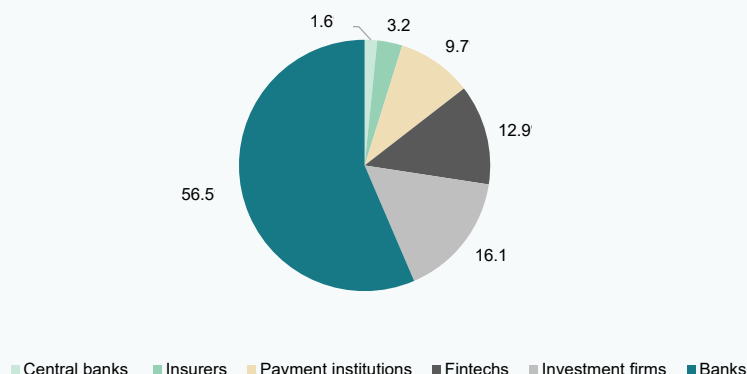
Exhibit 1 provides the breakdown of cyberattacks recorded in the European financial system based on information from EuRepoC. Banks account for 56.5% of the total number of attacks. At a considerable distance are investment service firms (16.1%), fintechs (12.9%), and payment institutions (9.7%). Insurers were victims of 3.2% of attacks and central banks 1.6%.

“ The first European annual report on major ICT-related incidents under DORA tallied 3,383 incidents in the European financial sector as a whole in 2025, around one-third of which had a cross-border impact. ”

Exhibit 1

Breakdown of cyberattacks in the European financial sector

Percentage



Source: Authors' own elaboration based on EuRepoC data.

Illegitimate access to an account or an employee's login credentials can facilitate transfers, fraud or extortion. The banks operate over large-scale digital infrastructure characterised by a high number of users and connections. The greater the number of access points, applications, interfaces and suppliers involved in provision of service, the larger the potential attack surface. The need to operate almost continuously increases the cost of attacks on availability, such as denial-of-service attacks or ransomware.

The outsourcing of services, use of shared software, cloud computing and connection with payment infrastructures create shared dependencies. A failure of or attack on a supplier can hit several institutions at the same time. The first European annual report on major ICT-related incidents under DORA tallied 3,383 incidents in the European financial sector as a whole in 2025, around one-third of which had a cross-border impact. System failures and external events were the

predominant driver of major incidents and nearly one-third originated from failures attributable to third-parties. In this context, digital resilience therefore requires tackling malicious actions, as well as ICT failures and ecosystem dependencies (European Supervisory Authorities, 2026a).

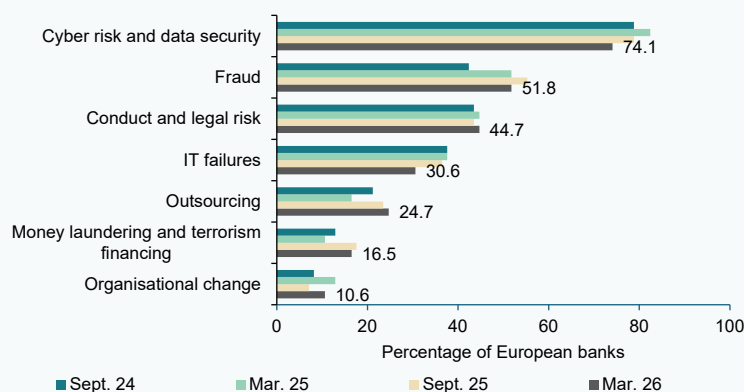
Cyber risk: Determining the operational risk and its materialisation

The perceived threat of cyber risk is evident in the responses provided by the banks in the EBA's six-monthly survey of 85 banks from the European Union and European Economic Space. Exhibit 2 illustrates the percentage of banks that identify the different sources of operational risk presented as a primary source of operational risk. The categories are not mutually exclusive: a given bank can view several sources of risk as relevant at the same time (EBA, 2026a).

“ In March 2026, 74.1% of the banks surveyed cited cyber risk and data security as a key operational risk driver, which was 22.3 percentage points ahead of fraud, mentioned by 51.8% of the banks. ”

Exhibit 2

Sources of operational risk (percentage of European banks surveyed answering in the affirmative)



Source: Authors' own elaboration based on EBA data.

In March 2026, 74.1% of the banks surveyed cited cyber risk and data security as a key operational risk driver, which was 22.3 percentage points ahead of fraud, mentioned by 51.8% of the banks. Behind fraud were conduct and legal risk (44.7%); IT failures (30.6%); and outsourcing (24.7%). Cyber risk and data security was identified as a key driver of operational risk by 78.8% of the banks in the September 2024 assessment, a higher 82.4% in March 2025, back to 78.8% in September 2025 and down to 74.1% in March 2026. The drop from the peak is tangible. Nevertheless, cyber risk ranked as the leading driver in all the assessments (EBA, 2026a). The reduction

in perceived cyber risk since March 2025 may reflect stabilisation in the number of attacks, reinforcement of defences, more mature risk management and DORA framework implementation.

Exhibit 3 depicts the trend in the percentage of European banks which fell victim to at least one cyberattack capable of provoking a major ICT-related incident in the previous six months. That percentage has been trailing lower, from 54.2% in September 2023 to 50.6% in September 2025 and 43.5% in March 2026 (EBA, 2026a). Despite the downtrend, the level remains high: in March 2026, more than four

“ Despite the reduction in the number of entities affected, from 54.2% in September 2023 to 43.5% in March 2026, the materialised losses derived from the latest cyber events have increased, reaching around 730 million euros in 2025, up from 650 million euros in 2024. ”

Exhibit 3

Percentage of European banks reporting having fallen victim to at least one cyberattack in the previous six months



Source: Authors' own elaboration based on EBA data.

out of every 10 banks faced at least one attack which resulted or could have resulted in a major incident in the previous six months.

Despite the reduction in the number of entities affected, the materialised losses derived from the latest cyber events have increased, reaching around 730 million euros in 2025, up from 650 million euros in 2024. These losses have also increased relative to common equity tier 1 (CET1) capital, albeit remaining at a low level on aggregate, at close to 0.04%. Accordingly, the direct costs of the cyberattacks would not appear to pose, by themselves, a significant threat to the European banks' solvency. However, the blended average may mask more significant impacts at certain entities and not fully reflect indirect costs such as the loss of business, customer payouts, reputational damage or the investments needed to restore and reinforce systems (EBA, 2026b).

The role of AI: Friend or enemy?

AI increases the banks' prevention, detection and response capabilities while at the same time providing attackers with more powerful and accessible tools. The relevant question is not, therefore, whether AI is intrinsically beneficial or harmful, but rather which actors are using it, to what end and framed by which controls?

On the defence front, AI systems can continuously analyse large volumes of logs, network traffic and transaction patterns to identify abnormal conduct that could be missed using static rules. They can also help prioritise alerts, detect malicious code, review software, summarise threat information and automate certain initial containment tasks. In terms of fraud, they can combine signals from multiple sources and adapt models for changing patterns. Their biggest advantage is the ability to process information at a speed virtually impossible for human teams to match, reserving expert intervention for the highest-risk cases (FSB, 2024 and 2026a).

The Anthropic case clearly illustrates this potential. In April 2026, the company unveiled Project Glasswing, a cybersecurity initiative using its unreleased frontier AI model, Claude Mythos Preview, to identify and correct vulnerabilities in critical global software. The initial partners included technology and cybersecurity players and one systemic financial institution: JPMorganChase. The participants using the model uncovered thousands of high-severity vulnerabilities, yielding a score of 83.1% on CyberGym, a vulnerability reproduction evaluation metric, compared to a score of 66.6% for Claude Opus 4.6. The initiative was articulated as a restricted-access research programme designed for defensive

Table 1 **Role of AI in cyber risk management**

Mitigator	Amplifier
Continuous analysis of logs, network traffic and transactions.	Automation and personalisation of attacks.
Capacity to prevent, detect and respond.	Speedy discovery and exploitation of vulnerabilities.
Prioritisation of alerts and ability to detect threats and fraud.	Use of social engineering to attack more effectively.
Review of software, summary of threats and automation of containment tasks.	Concentration of services at shared suppliers: correlation and contagion risk.

Source: Authors' own elaboration.

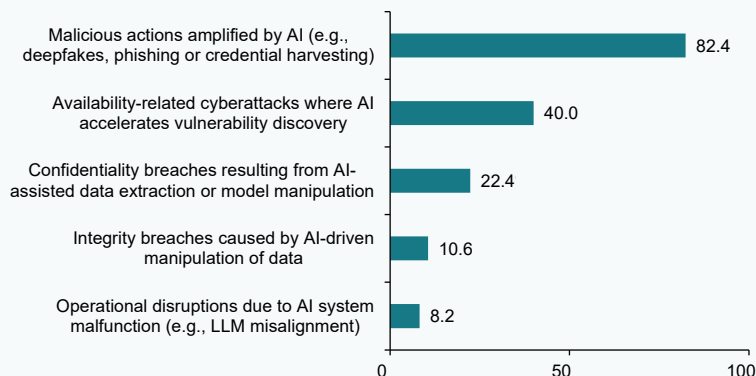
security use cases (Anthropic, 2026; Rodríguez Fernández, 2026). What is clear is that a model capable of detecting a vulnerability can help correct it but could also help facilitate its use by malicious actors. If the time needed to discover a flaw falls below the time needed by organisations to validate it, develop a patch and deploy it securely, the advantage could shift to the attacker.

Generative AI also lowers the barriers to social engineering. It can draft convincing and personalised messages in different languages, imitate communication styles and produce synthetic audio or video content.

This could increase the effectiveness of phishing campaigns, imitation of managers or suppliers or theft of credentials. The combination of the information obtained from open sources, stolen data and automated generation facilitates attacks targeted at specific employees with access to sensitive payments, systems or data. Deepfakes and other forms of imitation generated using AI show how the ICT risk could materialise through the manipulation of individuals and not necessarily via direct system intrusion.

Exhibit 4 shows how the European banks perceive the different ways in which AI could

Exhibit 4 **Percentage of European banks that believe that their vulnerability to the following types of ICT incidents could be amplified by AI**



Source: Authors' own elaboration based on EBA data.

“ The predominant concern relates to malicious actions enabled by AI, including deepfakes, automated phishing and credential harvesting, as cited by 82.4% of the banks. ”

amplify the adverse impact of ICT incidents. The predominant concern relates to malicious actions enabled by AI, including deepfakes, automated phishing and credential harvesting, as cited by 82.4% of the banks. This high percentage shows that the main fear is not yet autonomous model failure but rather AI's ability to render already familiar techniques more credible, scalable and effective.

Exacerbating the issue, many banks depend on a small number of cloud, model, hardware and software suppliers. The FSB has warned that AI could amplify vulnerabilities related to dependencies on third parties, cyber risk and model risk. If numerous banks use similar infrastructure, a failure or vulnerability can generate correlated effects. Management of AI cannot, therefore, be limited to validating each individual application but must also focus on identifying common dependencies, substitution options and continuity plans (FSB, 2024).

Conclusions

Cyber risk is high on European banks' agenda. AI can help them defend against this risk through better detection of anomalies, analysis of threats, identification of vulnerabilities and response times. However, it can also facilitate malicious uses. That is why it is not surprising that 82.4% of the banks believe that AI has the ability to amplify malicious actions, with 40% flagging the scope for denial-of-availability attacks and the exploitation of vulnerabilities.

The response should therefore be articulated around four principles:

- Prevention and shrinkage of the attack surface: updated software, strict access control and continuous vulnerability management.

- Speed of detection and response in line with the speed of the threat: permanent monitoring, defensive use of AI, skilled professionals and clear escalation protocols.
- Resilience *vis-à-vis* in-house and third-party failures: verified copies, proven recovery and exit plans around critical suppliers.
- AI governance: inventory of models, assessment of each use case, data quality and security, adversarial tests, traceability and human supervision proportionate to the gravity of the situation.

References

- ANTHROPIC. (2026). Project Glasswing: Securing critical software for the AI era. 7 April 2026.
- EUROPEAN BANKING AUTHORITY. (EBA). (2025). Risk Assessment Report. Autumn 2025.
- EUROPEAN BANKING AUTHORITY. (EBA). (2026a). Risk Assessment Questionnaire Results. Spring 2026.
- EUROPEAN BANKING AUTHORITY. (EBA). (2026b). Risk Assessment Report. Spring 2026.
- EUROPEAN SUPERVISORY AUTHORITIES. (2026a). 2025 Report on Major ICT-related Incidents.
- EUROPEAN SUPERVISORY AUTHORITIES. (2026b). Toward a Consistent and Risk-based Approach for ICT Risks from Frontier AI Models. 31 July 2026.
- EUROPEAN REPOSITORY OF CYBER INCIDENTS (EuRepoC). (2026). Database of Cyber Incidents.
- EUROPEAN UNION. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA).

FINANCIAL STABILITY BOARD (FSB). (2024). The Financial Stability Implications of Artificial Intelligence.

FINANCIAL STABILITY BOARD (FSB). (2026a). Sound Practices for Financial Institutions' Responsible AI Adoption: Consultation Report.

FINANCIAL STABILITY BOARD (FSB). (2026b). FSB Chair's Letter to G20 Finance Ministers and Central Bank Governors. August 2026.

RODRÍGUEZ FERNÁNDEZ, F. (2026). *Inteligencia artificial y estabilidad financiera: los riesgos bancarios en la era de la IA de vanguardia. Una evaluación comparativa de España, la Unión Europea y Estados Unidos* [AI and financial stability: Bank risks in the frontier AI era]. Investigaciones de Funcas, 40/2026.

Pedro Cuadros-Solas. CUNEF
University and Funcas

Nuria Suárez. Autónoma University of
Madrid and Funcas