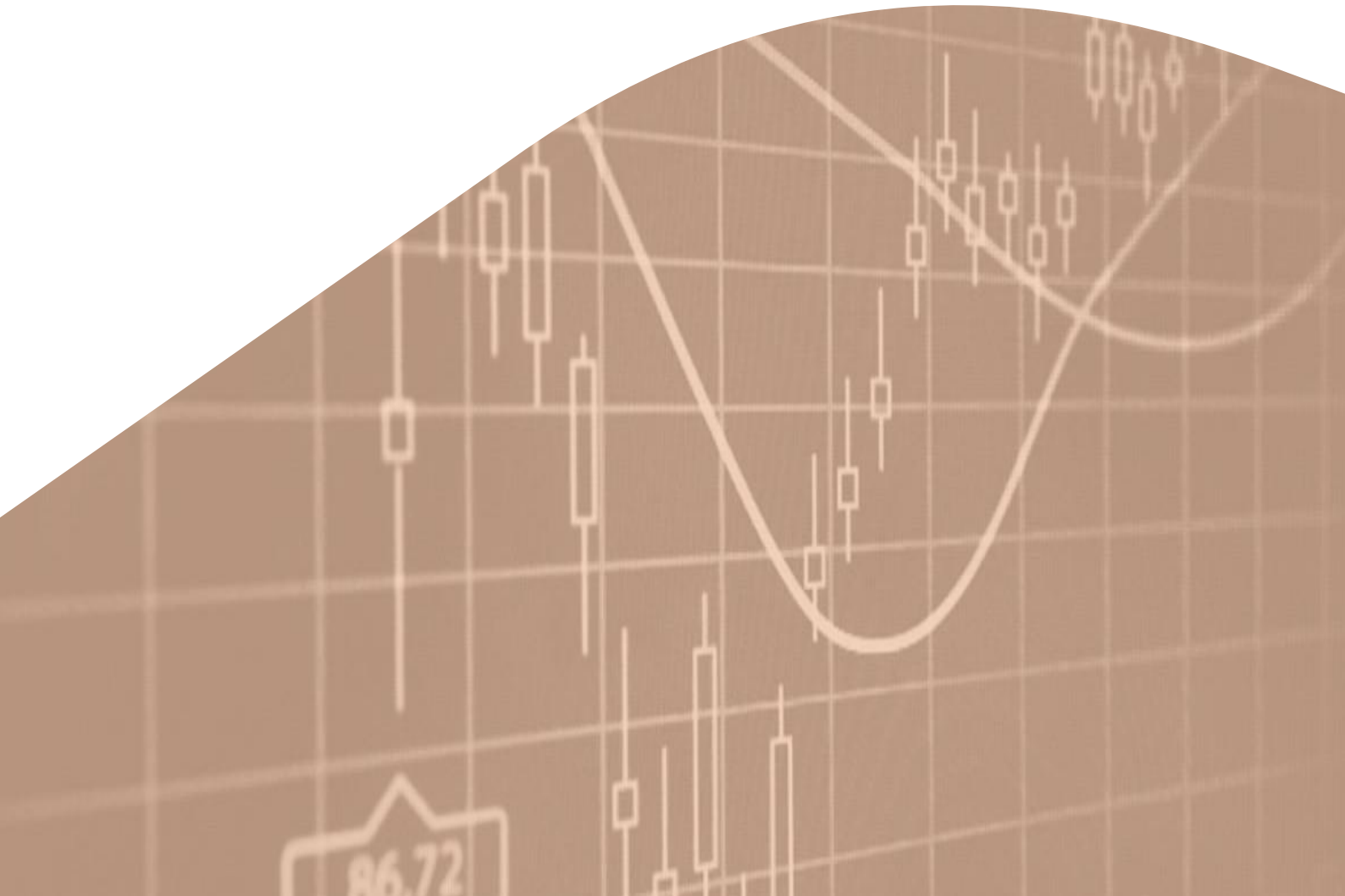
16 July 2025
ESMA50-1949966494-3823

ESMA TRV Risk Analysis

Financial Stability

Operational and cyber risks in EU financial markets: measurement and stress simulation



ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis

European Securities and Markets Authority (ESMA)
Economics, Financial Stability and Risk Department
201-203 Rue de Bercy
FR-75012 Paris
risk.analysis@esma.europa.eu
ESMA - 201-203 rue de Bercy - CS 80910 - 75589 Paris Cedex 12 - France - www.esma.europa.eu
Cover photo: Image Microsoft 365

Financial Stability

Operational and cyber risks in EU financial markets: measurement and stress simulation

Contact: onofrio.panzarino@esma.europa.eu[1] and steffen.kern@esma.europa.eu

Summary

Cyber risk has emerged as a growing threat to financial stability. The frequency and sophistication of incidents have increased in recent years, and their financial impact is both significant and growing.

Measuring and monitoring cyber threats from a financial stability perspective poses considerable challenges. The dynamic and rapidly evolving threat landscape, coupled with limited visibility into incidents, creates obstacles to accurate risk assessment and evaluation. In Europe, the Digital Operational Resilience Act (DORA) is set to have a concrete impact in terms of incident visibility. It introduced a harmonised, comprehensive framework for digital operational resilience for EU financial institutions and also established a reporting regime for major Information and Communication Technology (ICT) incidents by EU financial institutions.

This article delves into the systemic importance of cyber risk. It explores conceptual frameworks to examine how individual incidents can become systemic, by focusing on exposures to cyber threats, the propagation of the shock through the system, and their impact.

The paper also presents findings from a simulation analysis conducted on the EU repo market, examining scenarios in which a hypothetical cyber incident disrupts settlement operations at key market players. Results indicate that operational disruptions at a few critical institutions can trigger temporary yet severe liquidity shortages at both system and counterparty level, with widespread network effects.

The article underscores the need for robust cyber incident reporting frameworks, the development of risk metrics and monitoring tools on the basis of new sources of reporting data, and the use of conceptual models and simulations to enhance the assessment of cyber risks from a financial stability perspective.

The enhancements presented here will complement ESMA's operational risk monitoring framework.[2]

---

[1] This article was authored by Onofrio PANZARINO, Advisor in the Market and Payment Systems Oversight Directorate at the Bank of Italy, during a secondment to ESMA from May 2024 to April 2025. ESMA is grateful to Mr. Panzarino for his invaluable contributions to ESR's risk monitoring and analytical work.

[2] ESMA, "Operational risk assessment – the ESMA approach", ESMA Report on Trends, Risks and Vulnerabilities No. 1, 2018, pp. 68ff.

Introduction

Cyber risk is emerging as a growing concern for financial stability. Recent years have seen a steady increase in the number, scale, and complexity of incidents.[3] Malicious software and tools have become more sophisticated and increasingly available, allowing them to target vulnerable systems with greater ease and effectiveness. Financial institutions remain among the prime targets of cyber attacks.

Cyber risk differs from other types of operational risk in many ways and poses unique challenges. It arises from technological vulnerabilities and operational disruptions but can have far-reaching effects that extend beyond IT systems into more traditional risk categories, such as liquidity crises, contagion effects or widespread market disruption. Cyber risk is also complex to monitor and assess. Its dynamic, rapidly evolving nature, coupled with limited historical data, makes it difficult to accurately track and quantify.

This article examines these aspects in more detail and delves deeper into the importance of cyber risk from a financial stability perspective. The article is structured as follows:

- First, we explore the increasing frequency and scale of cyber incidents, the drivers behind these trends. We also explain the challenges for improved tracking and risk measurement and how cyber incident reporting under DORA will help mitigating these challenges.
- The second part of the article examines conceptual frameworks, modelling approaches and simulation analysis for assessing cyber risk and their impact on financial stability. It further presents a stress simulation exercise conducted on the EU repo market.

The enhancements presented in this article will complement ESMA's operational risk monitoring framework [4] and earlier work on operational resilience.[5]

Cyber risk as a growing threat to financial stability

Cyber risk can be defined as the combination of the probability of cyber incidents occurring and their impact on the financial system. Cyber incidents are malevolent or non-malevolent events that compromise the cybersecurity of IT systems or breach operational procedures and rules.[6]

Cyber risks have unique characteristics that distinguish them from traditional financial risks, such as market, credit, and liquidity risk.

- **Source of threat:** Cyber risks stem from digital threats targeting IT systems, infrastructure and data security – often due to technological vulnerabilities or malicious actors. Financial risks have economic causes such as market fluctuations, financial downturns, liquidity issues, or defaults.
- **Scope of impact:** The implications of cyber shocks can be widespread and extend beyond IT systems, affecting data integrity, business operations, reputation, and consumer trust. In contrast financial risks primarily influence profitability, investment returns, and economic conditions.
- **Risk monitoring and measurement:** In terms of risk monitoring, cyber threats require real-time surveillance, continuous security audits, and rapid-response mechanisms, while financial risks are typically assessed through periodic evaluations based on historical data and well-established financial models. More broadly, cyber risk management is dynamic and adaptive, responding to evolving threats, whereas financial risk assessment often relies on more structured and predictive frameworks, grounded on economic and financial theory.

Quantifying cyber risk remains notably difficult due to the ever-evolving threat landscape, limited historical data, and the complex interdependencies within financial systems. The following sections will explore these aspects in greater detail.

---

[3] See, e.g., ESRB (2024), ENISA (2024), ECB (2025).

[4] ESMA, "Operational risk assessment – the ESMA approach", ESMA Report on Trends, Risks and Vulnerabilities No. 1, 2018, pp. 68ff.

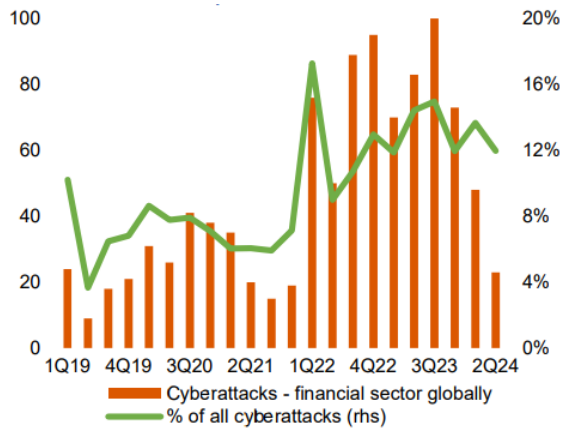
[5] ESMA, "A framework to assess operational resilience", ESMA Report on Trends, Risks and Vulnerabilities, TRV Risk Analysis, 19 December 2022.

[6] This definition of cyber risk is taken from the Cyber Lexicon developed by the FSB (2018).

Relevance, growth and drivers

The frequency and sophistication of cyber attacks have increased in recent years. Despite fragmented reporting and voluntary disclosures limiting comprehensive data availability, existing evidence consistently indicates an upward trend in cyber incidents, with an additional surge following the global COVID-19 pandemic. According to IMF (2024), the number of reported cyber incidents has nearly doubled since the onset of the pandemic. Data from other sources is showing the same trends. The ID Theft Resource Center (2020) reports 12,250 breaches over a 16-year period, with about half occurring in the last five years of this period. Data from the University of Maryland (the CISSM Cyber Events Database) further underscores that the number of cyber attacks has been historically high in the last five years (see Chart 1).

Chart 1
Cyber attacks on financial sector entities
Increased relevance of cyber events



Note: Cyberattacks on financial sector entities globally by quarter, publicly acknowledged incidents. For details, see Harry, C., & Gallagher, N. (2018). Classifying cyber events. Journal of Information Warfare, 17(3), 17-31.
Source: University of Maryland CISSM Cyber Attacks Database, ESMA.

Cyber threats continue to rank top among the risks identified by industry experts and regulatory authorities worldwide, and incident frequency is expected to climb further. Rating agencies have begun incorporating cyber risk into their credit assessments. A recent report by the European Union Agency for Cybersecurity (ENISA, 2024) also highlights a substantial increase in the variety of cyberattacks. This variety encompasses not only ransomware, which can cripple operations as exemplified later in the ICBC case study, but also other potent threats such as large-scale Distributed Denial of Service (DDoS) attacks aimed at disrupting service availability, sophisticated data breaches targeting the theft of sensitive customer or proprietary information, and increasingly prevalent attacks on the software supply chain which can introduce vulnerabilities across numerous interconnected entities. Each of these attack vectors can have distinct initial financial and operational impacts and follow different propagation mechanisms within the financial ecosystem, potentially requiring tailored preventative measures, detection techniques, and specific response strategies beyond general operational disruption planning.

The financial consequences of cyber incidents are significant and growing. Since 2020, cyber-related losses have totalled nearly USD 28bn, according to the IMF (2024). However, the wider costs of cybercrime could be far greater if indirect losses associated with the event, such as loss of trust and reputational damage, are also taken into account. [7] For instance, some studies (e.g., Jamilov, Rey and Tahoun, 2023) estimate the global cost of cybercrime to be as high as USD 200bn annually. However, figures vary significantly, reflecting challenges in precise quantification, differing methodologies, and scope of direct and indirect losses included. According to other studies, the estimated impact can range from 1 to 10 per cent of global GDP, with industry forecasts suggesting these costs will continue to rise in the future (see, e.g., Center for Strategic and International Studies 2020; ENISA, 2016; Statista 2022; Embroker, 2024).

Several factors contribute to the increasing frequency and severity of cyber attacks:

- **Expansion of digital connectivity:** The rapid growth of digital infrastructure has broadened exposure to cyber risks (see the section on "Ex-ante exposure to cyber threats" for a discussion of this aspect). The COVID-19 pandemic has further heightened dependency on technology and financial innovation, exposing vulnerabilities, especially with the rise of remote working.
- **Advances in cybercriminal techniques:** Malicious actors continue to develop and deploy more sophisticated tools, which are

[7] Direct losses include, for example, loss of business revenue due to operational disruptions, the amount of extortion or the amount spent to remedy the damage. Indirect losses include reputational damage, loss of future business and reduced productivity. See the following sections for more details on the distinction between direct and indirect losses.

also increasingly available for purchase by other individuals or groups, typically for financial gain (a model known as 'cybercrime as a service'), enabling a wider range of perpetrators to carry out attacks.

- **Geopolitical context:** Geopolitics continued to be recognized as a strong driver for malicious cyber operations (ENISA, 2024). Geopolitical risks are increasing and global conflicts and tensions, including Russia's invasion of Ukraine and unrest in the Middle East, have triggered spikes in cyber attacks.[8]

Financial institutions are among the most targeted entities,[9] as they typically handle large volumes of consumer data and significant assets, making them attractive to cybercriminals. Cyberattacks on these entities could cause in significant disruptions to society and economic activity.

Case study: The ransomware attack at ICBC Financial Services

On November 8, 2023, a ransomware group,[10] believed to be a highly sophisticated cybercriminal organization, managed to infiltrate the IT systems of the ICBC Financial Services (ICBC FS), a US-based financial services arm of the Industrial and Commercial Bank of China (ICBC). The subsidiary is wholly owned by ICBC and primarily engages in providing custody services to institutional clients, including global clearing, execution, and financing services.

The attack caused significant disruption to the bank's operations and interrupted its operating systems, including those used to clear US Treasury trades and repo financing transactions. This resulted in a temporary delay in its payment to counterparties. According to various press reports, the outage caused ICBC FS to temporarily owe BNY Mellon approximately USD 9bn, an amount far exceeding its net capital.[11]

Although the full extent of the event is not entirely clear, a Fitch Ratings (2023) analysis offered explanations as to why the disruption to the Treasury market from the attack was limited overall and did not affect its functioning (Reuters, 2023a). First, ICBC FS swiftly resolved outstanding payments shortly after the cyberattack, thanks to an emergency liquidity injection from its parent bank. Second, the size of ICBC FS is relatively small compared to its parent bank (0.4% of ICBC's total assets at end of the first half of 2023), whose primary business is in its core market in China. Additionally, the bank's segmented network architecture – with ICBC FS's systems operating independently from those of the parent group – also helped prevent the disruption from spreading more widely.

Despite the contained disruption in this instance, concerns remain that a similar attack on a financial institution lacking adequate shareholder support and emergency liquidity could trigger default events, with potentially significant financial stability implications.

Challenges and initiatives in cyber incident reporting

Despite the growing relevance of cyber threats as potential sources of systemic disruption, the general lack of information on cyber threats remains a key obstacle for both market participants and authorities in conducting comprehensive risk assessments and analyses.

Publicly available information on cyber events is generally scarce or of poor quality. This is largely due to reputational concerns, as firms face disincentives to voluntarily disclose operational failures that could undermine trust and harm their business. In addition, the lack of formal requirements to report cyber incidents in many jurisdictions exacerbates the problem. Available information on cyber events is also dispersed across multiple sources, making it even more difficult to obtain a comprehensive view of the cyber threat landscape. This is compounded by delayed reporting, which further distorts perceptions of the frequency and severity of incidents in most recent periods.

The lack of reliable data and information can lead to an underestimation of risk and the true impact of cyber events. Ultimately, this also leads to a reduced ability to take appropriate action to prevent or mitigate cyber threats.

---

8 See, e.g., IMF (2024).

9 According to some industry estimates (BCG, 2019), financial firms are 300 times as likely as other companies to be targeted by a cyberattack.

10 The breach was claimed by a cybercriminal group called Lockbit, which has in the past hacked some of the world's biggest organisations, stealing and leaking their sensitive data if they did not pay a ransom. According to US officials, it has become the world's largest ransomware threat (Reuters, 2024).

11 See, e.g., Reuters (2023b), The Banker (2023).

Improve tracking, risk monitoring and understanding of cyber threats

Information on cyber incidents is crucial for taking effective action and promoting financial stability (FSB, 2021). Lack of comprehensive data is indeed a critical impediment to effective supervision, financial stability assessments, and risk management at the firm level.

Efforts are underway at the global level to enhance operational resilience to cyber threats. Standard-setting bodies, financial regulators, and industry groups are combining their efforts to build more resilient systems, for example by developing policy guidance to strengthen cyber resilience, by considering cyber risks in internal or financial stability assessments, or in supervisory or internal stress exercises.[12] These initiatives address different aspects of cyber risk and contribute to its mitigation.

Given that cyber threats are inherently borderless and many large financial institutions and critical third-party providers operate on a global scale, effective international cooperation and coordination among regulatory and supervisory authorities are paramount. This includes striving for greater harmonisation of regulatory expectations where appropriate to avoid fragmentation and facilitate compliance for global firms, establishing clear protocols for cross-border information sharing during major incidents, and fostering international platforms for exchanging best practices in cyber resilience and threat intelligence to more effectively counter sophisticated global cyber adversaries.

Key initiatives also include the establishment of robust reporting frameworks that require organisations to provide timely and detailed reports on cyber incidents to the relevant authorities. These measures aim to address information gaps and foster collective action to tackle digital risks.

In Europe, the Digital Operational Resilience Act (DORA) is set to have a concrete impact in this area. It introduces a harmonised, comprehensive framework for digital operational resilience for EU financial institutions. It also established a reporting regime for major Information and Communication Technology (ICT) incidents by EU financial institutions. The framework covers relevant aspects of cyber events, including:

- The affected institution (including sector classification);
- The nature of the incident (e.g. cybersecurity-related, system failure, or external event);
- The date and time of the restoration of the services;
- The number of clients, counterparties and transactions affected by the incident;
- The financial costs and losses incurred;
- Whether the incident originated from a third-party service provider supporting critical business operations.

The reporting regime entered into force on January 17, 2025.

By establishing a standardised, mandatory reporting framework, the initiative has the potential to significantly improve the ability to identify, track, and understand cyber risks. It can also enable authorities to pinpoint systemic vulnerabilities, develop more accurate monitoring tools, and create risk indicators to track trends in cyber incidents across sectors and regions over time. Furthermore, it can provide valuable insights into contagion channels and system-wide vulnerabilities by analysing the intricate networks of ICT interdependencies between third-party service providers and financial firms. This allows for a better assessment of the financial system's resilience and responsiveness of the financial system to cyber threats, as well as how these threats evolve over time.

In addition to incident reporting, DORA encompasses other initiatives aimed at enhancing the EU financial sector's capacity to prevent, respond to, and recover from ICT disruptions. These initiatives also have the potential to facilitate more accurate cyber risk modelling and quantification. Examples include the reporting of significant cyber threats, the conduction of threat-led penetration tests, and the establishment of registers of ICT third-party service providers.

While DORA provides a comprehensive framework for digital operational resilience that extends beyond reporting, firms' proactive and continuously evolving defence measures remain

[12] To name but a few, the FSB (2018) developed a Cyber Lexicon to standardise communication on cyber risks. In the EU, the mandate of the European Network and Information Security Agency (ENISA) has been strengthened, and the European Supervisory Authorities (ESAs) have issued guidelines on ICT risk management. Various frameworks, such as the NIS Directive and TIBER-EU, address cyber risks. The ECB has established the Euro Cyber Resilience Board and conducted stress tests exercise on banks (ECB, 2024); the G7 has conducted cross-jurisdictional cyber exercises.

crucial. These include sustained investment in advanced security technologies such as AI-driven threat detection systems and anomaly detection, regular and rigorous testing to proactively identify and remediate vulnerabilities, the development, testing, and regular updating of robust business continuity plans (BCP) and incident response plans (IRP), and comprehensive, ongoing cyber hygiene training for all staff. Moreover, fostering platforms for timely, voluntary threat intelligence sharing among financial institutions can complement formal reporting mechanisms and enhance collective situational awareness and preparedness.

Models for analysing systemic cyber events

Cyber threats have increasingly come into focus as a significant risk to financial stability, as highlighted in previous sections. Economists, market participants, and financial authorities continue to highlight the urgent need to deepen understanding of cyber-related threats and build capacity to assess their impact from a systemic perspective (Duffie and Younger, 2019; Kashyap and Wetherilt, 2019).

Over the years, several conceptual models have been developed to explore how single events can escalate into a systemic threat and to better navigate the complex web of mechanisms and linkages at play in modern financial ecosystems. Notable examples that build on prior research[13] include ESRB (2020), ECB (2025) and IMF (2024).

According to many studies, the development of a cyber shock can generally be broken down into three stages:

(1) the exposure to cyber threats;

(2) the release of the shock and its propagation through the financial system; and

(3) the resulting macroeconomic and financial consequences, which affect key economic functions.

Each stage is discussed in detail in the following sections.

Ex-ante exposure to cyber threats

The first aspect to consider when studying a cyber event is the firm's vulnerability to this risk, i.e., its ex-ante exposure. In principle, individual firms have different layers of exposure to cyber risks, depending on a range of factors. These may be firm-specific or external.

Firm-specific factors relate to the individual characteristics of each firm. For example, firms with a greater digital presence, e.g. if their core business relies heavily on new technologies or requires high technological connectivity, may be more vulnerable to cyber threats. Conversely, proactive measures, such as investing in cybersecurity, training employees and raising awareness of cyber hygiene[14] can reduce the 'surface area' of exposure to cyber attacks and mitigate risks.

External factors include the geopolitical context and the regulatory environment. Companies operating in regions with geopolitical tensions may be more exposed to cyber attacks (IMF, 2024). Similarly, jurisdictions with less mature cyber laws can lead to higher vulnerability for firms.

Both layers of exposure evolve over time, influenced by shifts in technology development and adoption. While these advances can be beneficial for innovation and consumer services, these can also inadvertently increase exposure to cyber threats.

Shock release and transmission

The second phase focuses on the release of cyber shocks and their amplification across the financial system. Cyber events, as defined by FSB (2018), refer to occurrences – malicious or not – triggered within IT systems or networks. Once triggered, a cyber event can develop into more traditional risks, such as liquidity crises and financial contagion, and threaten financial stability through several channels.

First, the temporary unavailability of financial services provided by critical entities in the financial system can lead to market dysfunction, given the potential lack of ready substitutes.

Second, a loss of confidence can erode trust in institutions and financial markets, leading to 'run-like' behaviour and increased liquidity risks; for example, through deposit withdrawals or bank runs, also referred to in this context as 'cyber

[13] See, e.g., Ross (2020), Kaffenberger and Kopp (2019), Healey et al. (2018), and Brando et al. (2022).

[14] This means online security and system health practices such as anti-malware and multi-factor authentication.

runs' (Duffie and Younger, 2019). A loss of confidence can have a domino effect, triggering potentially contagious channels and asset fire sales, even in institutions not directly affected (Brando et al., 2022).

Third, disruptions in one part of the system may spread to others, leading to contagion effects and broader financial instability. In the case of cyber events, the channels through which the shock may be transmitted may involve not only business ties (e.g., trading relationships, commercial links) but also more complex and often unrecognised links between firms, including a layer of exposure to shared technologies and third-party service providers. Third-party service providers and their interconnectedness with other financial institutions and market infrastructures add a new layer of interdependencies that can exacerbate vulnerabilities. Incorporating these types of relationships is critical when conducting risk assessments (Bouveret and Herraez, 2022).

Impact

The third stage evaluates the point at which a cyber event can have a systemic impact. Financial stability depends on the ability of the financial system to provide key economic functions (KEFs) in the event of a cyber incident (ESRB, 2022). This phase considers whether a cyber incident adversely affects macroeconomic outcomes to the extent that the system is no longer able to provide a KEF and 'absorb' or mitigate the shock. Examples of KEF impairments include a reduction in the provision of credit, disruption of critical financial services such as payment or settlement systems, crystallisation of a systemic financial shock such as liquidity shortages or impaired market functioning.

Authorities can employ impact thresholds to quantify resilience. The upper threshold defines the maximum impact the financial system can withstand, while the lower threshold indicates the minimum operational level for institutions and functions. The space between these thresholds reflects the system's capacity to absorb shocks and maintain stability (ESRB, 2023). Identifying these thresholds can enable authorities to assess the resilience of their firms, financial market infrastructures and markets, and support the development of crisis response, coordination and intervention capabilities. Work is underway to develop approaches for identifying these thresholds.

To better illustrate how a cyber event can develop into a systemic risk, the above model has been applied to a simulation exercise focusing on the European repo market. The analysis is presented in the following section.

Risk measurement and stress simulations

As highlighted, the impact of cyber incidents can be far-reaching, potentially disrupting critical market functions and developing into a financial stability risk.

Assessing the systemic relevance of cyber threats is key from a financial stability perspective and requires an indication of the magnitude and criticality of potential losses in the event of cyber-related disruptions. Recent research, such as Bouveret (2019), highlights frameworks to quantify cyber risk. These studies demonstrate how models used for operational risk assessment in banks can be adapted to analyse cyber risk. The results indicate that estimated losses can be substantial, especially when compared to the size of the cyber-insurance market, and the distribution of these losses can exhibit heavy tails.

More generally, modelling frameworks and stress simulations can be powerful tools for exploring these aspects and, in the context of risk assessments, can provide useful insights into:

- **Shock materiality,** by providing a detailed assessment of the operational disruption and potential financial impact that could result from a cyber incident. This quantification is critical to understanding the magnitude of the threat and preparing appropriate mitigation strategies.
- **Amplification channels,** as cyber incidents can propagate through interconnected systems and markets, amplifying their impact. Simulation analysis can help identify these channels and provide a better understanding of how a localised incident can escalate into a systemic risk.
- **Ex-ante vulnerabilities,** by simulating scenarios that allow financial institutions and authorities to pinpoint weaknesses in the system. This proactive approach enables the strengthening of defences and the enhancement of overall system resilience.

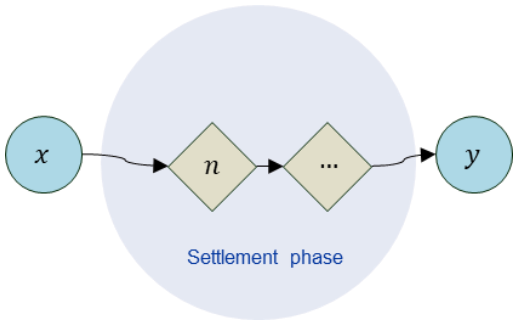
The modelling approaches adopted in this study also align with the broader ESMA (2018) operational risk strategy, complementing qualitative operational risk assessments with analytical frameworks that can map propagation channels and systemic linkages. This is particularly important when cyber risk manifests

through infrastructure-level disruptions and third-party dependency. Simulation-based analysis offers a forward-looking quantification of exposure to cyber events and could serve as a prototype for developing future quantitative indicators of operational risk.

The next section presents a simulation exercise designed to study the potential impact of a cyber event affecting the functioning of the repo market in Europe. The analysis revolves around the design of a hypothetical cyber shock that disrupts the settlement of repo transactions, similar to the ICBC FS cyber incident in the US Treasury market in November 2023 (see previous sections).

The following sections outline the context for the simulation exercise, the scenario designed, the approach to risk measurement, and the results of the analysis.

Chart 2
Market setting
Stylised repo transaction



Note: Illustration of a repo transaction between two counterparties, where one entity (i.e. the repo borrower, *y*) receives funding from another market participant (i.e. repo lender, *x*). Diamonds (e.g., node n) represent settlement nodes in the post-trade phase of the transaction. They are direct CSD participants handling settlement operations and can be either the counterparty itself or a third-party service provider. They are the targets of the cyber-attack considered in the analysed stress scenario.
Source: ESMA.

Stress simulation: Evidence from the EU repo market

Repo markets are critical from a financial stability perspective. They fulfil several functions, ranging from the provision of liquidity to a wide range of investors to the exchange of collateral in the financial system, thereby supporting the functioning of markets and the wider economy.

This analysis uses regulatory data from the Securities Financing Transactions Regulation (SFTR), which provides detailed and granular information on repo and reverse repo transactions conducted by market participants in Europe. A comprehensive overview of the EU repo market, based on information reported by market participants under SFTR, is provided in ESMA (2024).

Market setting

Our simulation exercise builds on scenarios where a cyber event affects an institution's ability to settle its repo transactions on a given day and investigates quantitatively the resulting impact on the wider repo network.

The reference market setting for the analysis is illustrated in Chart 2. It shows a stylised example of a repo transaction between two counterparties, where one entity (i.e. the repo borrower, y) receives funding from another market participant (i.e. repo lender, x). Once the trade has taken place, it must be settled by means of delivering securities and making cash payments between the parties. Settlement is not complete until the repo lender and the borrower have fulfilled their mutual obligations, i.e. the delivery of securities for the repo borrower and the cash payment for the lender.

The management of post-trade tasks is generally handled by the operations departments of the trading counterparties (see ICMA, 2023). For settlement purposes, they send instructions to deliver and receive securities to Securities Settlement Systems (SSSs), which are operated by domestic central securities depositories (CSDs) or international central securities depositories (ICSDs). Transactions are generally settled on a delivery versus payment basis, i.e. a mechanism that connects the transfer of securities to the transfer of cash in such a way that the delivery of securities takes place if and only if the corresponding transfer of cash occurs, and vice versa. Consequently, if a counterparty fails to deliver either the securities or the cash, the transaction is not settled.

Settlement nodes and third-party dependencies

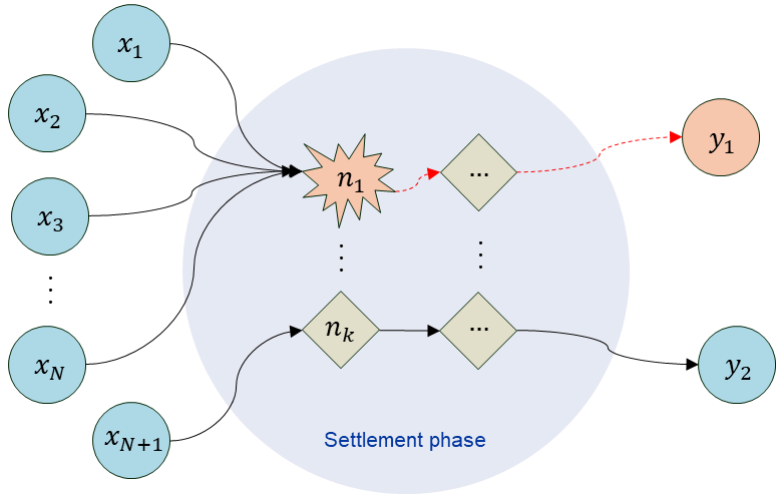
Direct participation in CSDs is subject to financial, operational and legal constraints that can be burdensome and costly for market participants. Investing in multiple markets would also require an account in different CSDs. Instead of direct access to CSDs, investors may choose to rely on settlement services provided by a third party,

such as a custodian banks,[15] to settle their transactions. For the purposes of this analysis, the entities that handle the settlement processes on their own behalf and/or on behalf of their clients are referred to as settlement nodes.

A unique feature of the dataset used in this analysis is that it allows the identification and mapping of the critical settlement nodes in the European repo network. EU entities report whether they are direct members of a CSD or instead rely on a third party to settle their transactions, i.e. the so-called indirect CSD participation model. In the latter case, reporting entities provide details to identify the third-party providing the services (i.e. LEI code; for reference, see ESMA, 2021).

Settlement nodes are shown as diamonds in Chart 2 (e.g., node n). As mentioned above, they refer to direct CSD participants that handle settlement operations and can be either the counterparty itself or a third-party service provider. These entities are the target of the cyber-attack considered in the analysed stress scenario.

Chart 3
Repo settlement network: a stylised example
Cyber shock in the analysed scenario



Note: Stylised example of a repo settlement network displaying settlement nodes and third-party dependencies. In the stress scenario analysed, the node n_1 experiences a cyber incident that temporarily affects its ability to settle transactions. As a result of the incident, repos negotiated by entities $x_1, x_2 \ldots x_n$ are not settled as expected and entity y_1 experiences a temporary liquidity shortage, i.e. the cash borrowed through repos does not reach its balance sheet as planned.
Source: ESMA.

By using information on critical settlement nodes in the repo network, our analysis can identify stress scenarios where a counterparty that receives funding from different entities, but through a common settlement node, may be more affected by the event. Interconnectedness is widely recognised as a key factor in financial stability risk assessments. As discussed in previous sections, cyber shocks can propagate through linkages that go beyond business relationships, such as through third-party service providers. This adds a new layer of interdependencies that can spread shocks and exacerbate vulnerabilities.

The funding provided by otherwise unrelated repo lenders may be affected by the same IT incident if, for example, the two entities rely on the same settlement node. The analysis takes this potential channel of contagion into account.

Baseline scenario

As highlighted, the stress simulation focuses on a scenario where a hypothetical cyber incident

[15] Custodians provide a wide range of services, including settlement, custody, and all general post-trade operations related to the life cycle of financial securities. For further reference on the business model of custodian banks and the role they play in modern financial ecosystems see Coste et al. (2021).

affects the ability of a critical settlement node to operate. For example, a cyber-attack may temporarily affect the availability of relevant data or communication and messaging systems of a target institution, such as, in this case, a primary bank providing post-trading services to investors, which may be temporarily unable to process or transmit payments to SSSs.

In the designed scenario (baseline), the cyber-attack targets one of the 10 largest settlement nodes in the European repo network. Settlement nodes are direct CSD participants as defined in the previous paragraph. It is assumed that, once affected by the cyber-hack, the node would be unable to settle all repo transactions with its counterparties, either on its own account or on behalf of its clients (in the case of intermediaries providing custody services, such as custodian banks).

Although the designed scenario focuses on a targeted cyber-attack, it is important to note that the stress simulation and its results would remain valid if the outage were caused by a general operational incident. These could include, for example, computer system failures, human error, or other unforeseen events that similarly interrupt the entity's ability to settle transactions. Therefore, the main findings of the analysis can be interpreted as covering a wider range of potential operational disruption risks and impacts, instead of cyber-attacks specifically.

Chart 3 provides a stylised example of the baseline scenario described above. Node n_1 experiences a cyber incident that temporarily affects its ability to settle transactions. As a result of the incident, repos negotiated by entities $x_1, x_2 \ldots x_n$ are not settled as expected and entity y_1 experiences a temporary liquidity shortage, i.e. the cash borrowed through the repos to be settled that day does not reach its balance sheet as planned.

Conversely, the securities provided as collateral in the repos are also not exchanged between the parties and remain (unencumbered) on the balance sheet of the collateral provider (y_1 in the example). While this paper focuses on the liquidity channel, the collateral side can also be explored as a potential source of systemic risk, as large settlement failures might undermine the liquidity and smooth functioning of securities markets (see, for example, Iyer and Macchiavelli, 2017). This aspect is left for future research.

A caveat to this analysis is that the duration of the incident may be limited in time and IT operations may be quickly resumed, for example if the target institution has effective operational contingency plans in place. In addition, the failure is assumed regardless of the likelihood of the failure to occur.

While this stress simulation focuses on the immediate impact of a cyber incident, a broader assessment must consider additional factors. These include the ability of firms to restore their IT systems, the likelihood of the incident occurring, and the availability of business replacements. Different institutions may have varying speeds and capacities for recovery, and prolonged disruptions could worsen initial impacts. It's also crucial to consider how other market participants might react, such as hoarding liquidity, fleeing to safer assets, unwinding positions with affected counterparties, or even fire sales if liquidity pressures increase. The initial shock could propagate further through these behaviours. Conversely, mitigating actions like activating comprehensive business continuity and crisis management plans, coordinated industry responses, or finding business replacements could change the event's trajectory after the initial impact.

Although these factors are important for risk assessments, they are often hard to observe and may need further modelling and hypotheses. Additionally, the underlying information can be scarce or inaccurate, making it difficult to provide reliable estimates (see previous sections for further discussion of data gaps in cyber risk modelling).

In any case, in the scenario analysed, the operational failure would have an immediate and direct impact on the ability of institutions to carry out their day-to-day business and, for a period of time, the inability to process or transmit payments would lead to a temporary shortage of liquidity for counterparties. In the next section we focus on quantifying this potential impact.

Empirical approach

The target of the stress simulation is to analyse scenarios in which a cyber incident prevents one of the largest participants in the repo market from settling its trades and to quantify the potential liquidity impact of the shock on the repo network.

As highlighted in previous sections, cyber incidents can morph into more traditional financial risks and develop into a systemic event by affecting the provision of key economic functions, such as the supply of credit or the provision of critical services by a financial market infrastructure. This analysis focuses on one particular KEF: the provision of funding through repos and the impact of a cyber incident that disrupts the settlement of repos for a subset of critical institutions, resulting in a temporary lack of liquidity for a number of counterparties.

In order to assess the magnitude of the potential liquidity impact of the cyber shock, we take the following steps. First, we identify the set of the 10 largest settlement nodes in our sample (in terms of total gross settlement amounts). For this analysis, settlement nodes are defined as direct CSD participants. They are the targets of the cyber-attack in the scenario (referred to as 'affected nodes'). Second, for all counterparties connected to each affected node, their net repo borrowing position is computed using the following formula:

$$Repo_{t,n,i} - Rev.Repo_{t,n,i}$$

where $Repo_{t,n,i}$ $(Rev.Repo_{t,n,i})$ is the outstanding amount (in billions of EUR) of repos (reverse repos) to be settled at the beginning of day t by counterparty i and through settlement node n.

Third, in order to quantify the impact of the shock, the following risk indicators were taken into account:

- **Liquidity shortage,** calculated as the sum of total net repo borrowing affected by the shock, at system and counterparty level (and expressed in EUR bn).
- **Relative liquidity shortage,** calculated as the share of repo borrowing affected by the shock, at system and counterparty level (and expressed in percentages).
- **Number of affected (or 'impaired') entities,** i.e. counterparties for which a portion (or a significant share) of their total borrowing on the repo market borrowing is affected by the cyber shock (and therefore not settled when expected).

To capture a larger number of potential outcomes and add robustness to the results, the simulation has been repeated for 100 randomly selected trading days, and for each, it was repeated across the 10 major settlement nodes (resulting in 1,000 scenarios). The findings of the analysis are presented in the next section.

Table 1
Simulation results, descriptive statistics
Impact material and widespread across repo counterparties

	Mean	SD	p5	p10	p25	p50	p75	p90	p95
					System level				
Liquidity shortfall, EUR bn	35.2	32.8	0.4	1.1	7.7	25.5	64.8	87.5	96.3
Share of affected borrowing, %	6.2	5.7	0.1	0.2	1.4	4.6	11.8	15.1	16.6
Num. of affected counterparties	64.1	58.6	6.0	7.0	12.0	61.0	88.0	127.1	198.0
Num. of impaired counterparties	31.3	38.5	1.0	2.0	4.0	20.0	43.0	78.0	124.0
					Counterparty level				
Liquidity shortfall, EUR mn	735.3	1,923	0.5	1.2	8.0	130.1	541.2	1,767	3,347
Share of affected borrowing, %	47.6	39.7	0.1	1.0	8.6	38.9	100.0	100.0	100.0

Note: Descriptive statistics on the distribution of liquidity shortfalls and the number of affected entities, resulting from a cyber event targeting one of the 10 largest participants (nodes) in the RSN. Impact indicators are computed at the system and at the counterparty level. The simulation is conducted over 100 randomly selected days, from January 2023 to June 2024.
Source: SFTR, ESMA calculation.

Results

Results are shown in Table 1 and Chart 4. According to the stress simulation analysis, the disruption of settlement operations at any of the 10 largest participants in the EU repo settlement network would have been associated with a substantial liquidity shortage, of about EUR 35bn, on average at the system level.

The impact is non-negligible when compared, for example, to the total funding in the repo market. The results show that, on an average day in our sample, around 6% of the total repo borrowing is potentially affected by the incident. The financial impact of the cyber shock can be particularly severe in most adverse scenarios. As shown in Chart 4, the impact distribution has a long right tail, and the magnitude of the impact can almost triple to over 16% of total borrowing in most extreme cases (95th percentile). This finding is also consistent with previous studies showing that losses due to cyber risk can be heavily skewed (Bouveret, 2019).

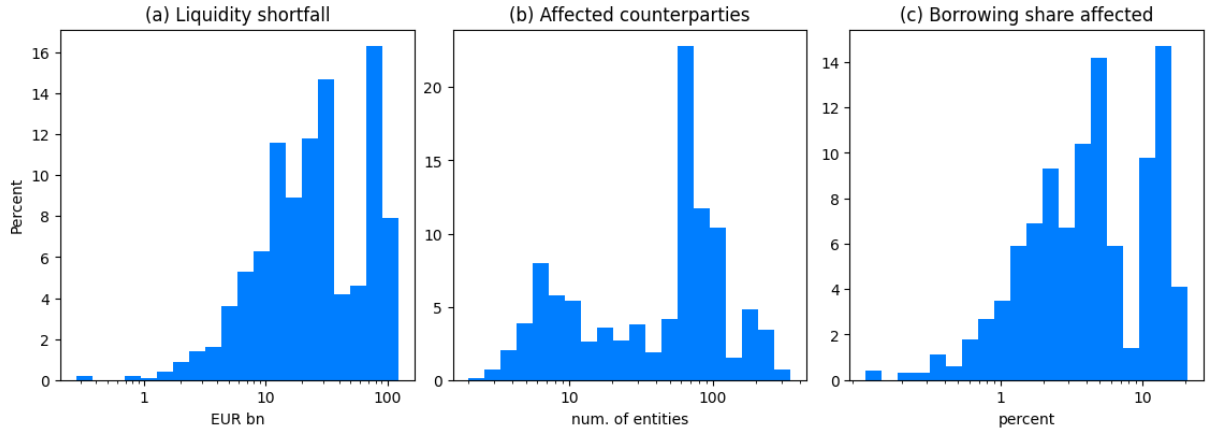
The potential liquidity shock is also generally widespread across entities, potentially affecting several counterparties. On average, more than 60 repo borrowers are involved in the incident, rising to well over 100 in most adverse scenarios.

The average impact at the counterparty level is estimated at around EUR 750mn. The figure is high and affected by the presence of outliers: according to the simulation results, the median value of the individual impact is much lower and indicates that in half of the cases the shock could be as much as five times smaller (i.e. below EUR 150mn).

To look more closely at the impact of the cyber shock at the firm level, Chart 5 shows the distribution of the potential liquidity shortfall that repo counterparties may face in the stress scenarios analysed. The distribution of the impact is broken down by counterparty sector (Chart 5, panel b), by direct or indirect participation in CSDs (i.e. when repo funding is provided by lenders that do or do not rely on third parties providing settlement services; Chart 5, panel c), by the share of the firm's borrowing affected by the event (at the firm level; Chart 5, panel d).

The estimation results highlight the following. First, the IT incident may have a widespread impact across sectors, leading to spill-over effects on several counterparties, with primary banking institutions (such as dealers) and CCPs being the most affected. The temporary liquidity shortfall may exceed EUR 10bn at the individual level under certain scenarios (see Chart 5, panel b), reflecting for instance the 'network centrality'[16] of some entities in the EU repo network, as well as the overall level of interconnectedness and concentration in the market (see e.g. ESMA, 2024).

Chart 4
Simulation results, impact distribution
Temporary liquidity shortages can be large at the system-level



Note: Distribution of impact resulting from simulation results, based on a stress scenario of a cyber incident disrupting one of the 10 largest participants (nodes) in the EU repo settlement network. Simulation conducted over 100 randomly selected days, from January 2023 to June 2024. Impact indicators calculated at the system level (across counterparties of each 'affected node'): liquidity shortfall in EUR bn (panel a), number of affected entities (panel b), affected share of borrowing (panel c).
Source: SFTR, ESMA calculation.

Second, as highlighted, this stress simulation uses information on critical settlement nodes - i.e. entities that are direct participants to CSDs and settle repo transactions on their own or their clients' behalf - to examine other potential channels of contagion following a cyber incident.

Chart 5 (panel c) shows that, in a quarter of cases, affected counterparties borrow cash from entities that rely on a third party to settle their repo transactions.

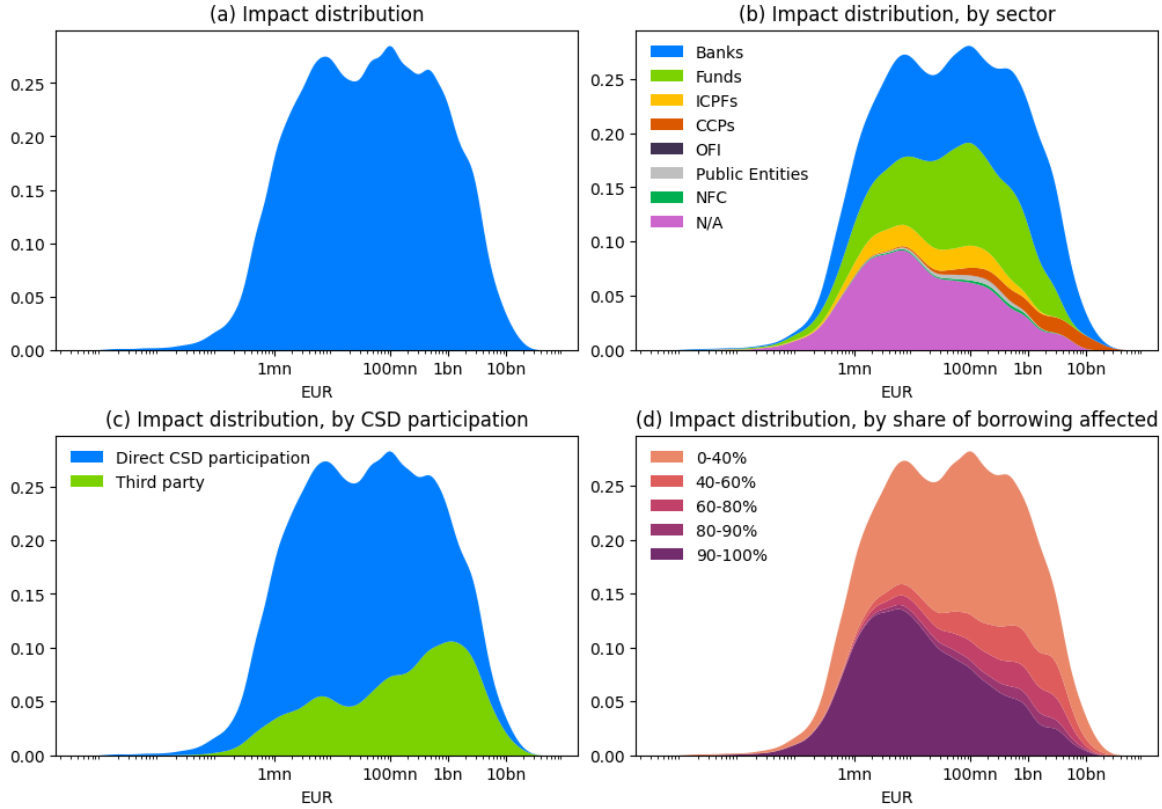
The results also highlight that this channel can transmit significant liquidity shocks through the

[16] A network analysis conducted by ESMA (2024) illustrates the existence of a core-periphery structure in the EU repo market, highlighting the intermediation role of banks (at the core) through which a variety of counterparties from different sectors access the repo network. By design, the centrally cleared segment shows a star-shaped pattern - or rather several star-shaped patterns around several CCPs, with significant exposures flowing through a few core CCPs and a few large clearing members.

system: counterparties that receive repo funding from entities dependent on third-party settlement can experience a temporary liquidity shortage of significant size (i.e. as illustrated by the skewed green area prominently positioned on the right-hand side of the chart). This may reflect that counterparties receiving funding from various entities, but via a shared settlement node impacted by the cyber shock, are likely to experience a large impact since the settlement operations of all these lenders would be affected by the same incident. The analysis thus identifies settlement hubs and third-party dependencies as critical channels of contagion.

Thirdly, while the liquidity impact on individual entities can be significant in absolute terms, it may account for only a small proportion of counterparties' total repo activity. According to our results, when a counterparty is affected by the incident, in 25% of cases the impact concerns less than 9% of its total repo borrowing (see Table 1).

Chart 5
Simulation results, impact distribution
Broad impact across sectors and different channels of contagion



Note: Distribution of the liquidity impact calculated at the counterparty level and resulting from a stress simulation where a cyber incident disrupts one of the 10 largest participants in the EU repo settlement network. The impact is computed in terms of the temporary liquidity shortfall that counterparties may face in the analysed scenario and is calculated as the sum of the total net repo borrowing affected by the incident (and expressed in EUR bn). The distribution of the impact is broken down by counterparty sector (panel b), by direct or indirect participation in CSDs (i.e. if repo funding is provided by lenders that rely on third parties to provide settlement services or not; panel c), according to the share of the firm's borrowing affected by the event (panel d). Simulation conducted over 100 randomly selected days, from January 2023 to June 2024.
Source: SFTR, ESMA calculation.

The limited share of total funding affected by the disruption may indicate that counterparties have a broad network of repo relationships to support their funding needs. All else equal, a broader repo network may increase resilience to shocks by allowing institutions to obtain funding from alternative repo lenders (via unaffected settlement nodes). Chart 5 (panel d) illustrates this point further and shows that, in general, the larger the liquidity impact, the smaller the share of borrowing affected (and vice versa). The finding suggests that large(r) market participants

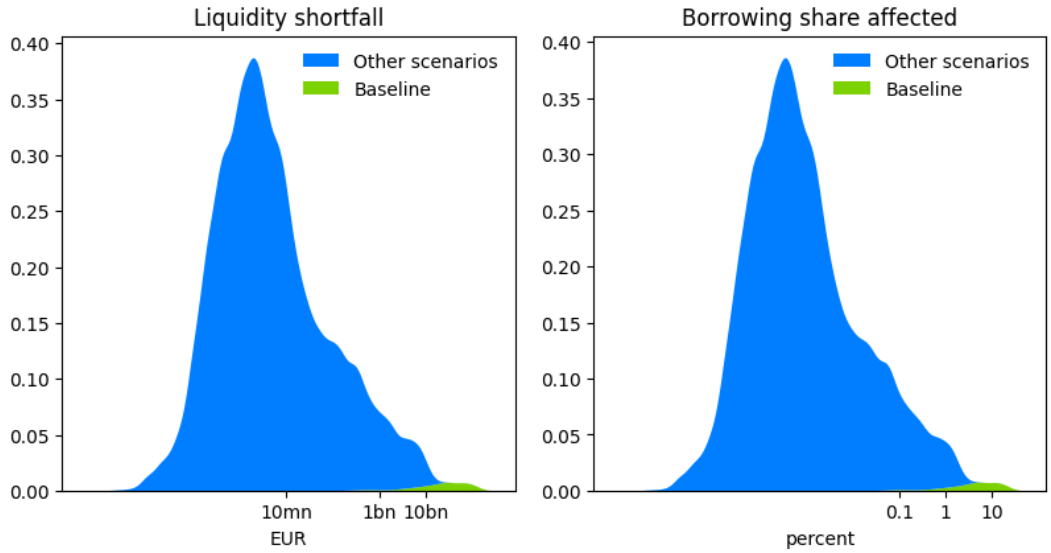
facing potentially bigger impacts tend to have wider networks and more diversified repo funding sources. On the other hand, the result also suggests that in the case of less significant impacts, e.g. associated with thinner exposures of smaller firms, the share of borrowing affected by the incident is instead high, presumably reflecting the less developed repo networks of some firms that rely on a relatively small number of dealers to meet their funding needs.

In principle, a comprehensive risk assessment should not focus solely on the magnitude of the potential impact. For example, larger or more sophisticated institutions may have more resources, contingency plans or buffers to deal with temporary disruptions or liquidity shortfalls than other market participants. Factors such as the institution's size, sector, balance sheet strength, contingency planning, risk management practices and regulatory requirements also play an important role in risk assessments.

Reverse stress test

The results of the simulation analysis showed that a successful cyber-attack at any of the 10 largest settlement nodes in the EU repo network could have a far-reaching impact on the system. As highlighted, these nodes are generally large institutions that are direct participants in CSDs and settle large volumes of repo transactions on their own behalf or on behalf of their clients (as in the case of custodian banks).

Chart 6
Reverse stress test
Additional risks from 'less-critical' settlement nodes



Note: Impact distribution from a reverse stress simulation, considering a hypothetical cyber incident on any of the settlement nodes in the repo network (including at the top 10 nodes, i.e. the baseline scenario; green area). Simulation over 100 random days (Jan 2023–Jun 2024). Liquidity shortfall calculated at system level (log scale).
Source: SFTR, ESMA calculation.

These major institutions can benefit from economies of scale in cybersecurity investment and may be subject to more stringent regulatory oversight and requirements, further strengthening their defences. As a result, cyber attacks are likely to be more successful when targeting institutions with weaker security frameworks, looking for vulnerabilities that are easier to exploit. Smaller institutions might lack the extensive resources needed to defend against sophisticated attacks, leaving them more vulnerable to breaches.

A reverse stress test was conducted to assess whether an attack on less critical nodes in the network could still pose a significant threat to financial stability. A larger set of calculations was performed to quantify the potential liquidity shortfall resulting from a hypothetical cyber-attack targeting any of the settlement nodes in the system.

Chart 6 summarises the results, illustrating the system-wide distribution of potential liquidity shortfalls caused by a successful attack on each node within the repo network. This reverse simulation also takes into account disruptions at

the 10 largest settlement nodes previously examined in the baseline scenario, thereby extending the scope of the analysis. The impact associated with these nodes is highlighted in the green area of Chart 6.

In the baseline scenario – where an attack targets one of the 10 largest settlement nodes – the adverse effects are most severe, as shown by the green area in the right tail of the impact distribution. The analysis underscores that operational disruptions at these critical nodes could trigger significant liquidity shortages at the system level, leading to worst-case outcomes.

However, successful cyberattacks on less critical settlement nodes can also result in significant impacts. For example, our findings indicate that an incident at a node processing less than one-tenth of the average flows settled by a major node could lead to substantial system-wide liquidity impacts amounting to around EUR 5bn or more (approximately 1 per cent of total repo borrowing in the analysed scenarios). These results highlight that even small-scale attacks can have systemic implications when amplified by network interconnectedness.

Conclusion

Cyber risk has emerged as a growing threat to financial stability. The frequency and sophistication of incidents have increased in recent years, and their financial impact is both significant and growing.

Measuring and monitoring cyber threats from a financial stability perspective poses considerable challenges. The dynamic and rapidly evolving threat landscape, coupled with limited visibility into incidents, creates obstacles to accurate risk assessment and evaluation. In Europe, the Digital Operational Resilience Act (DORA) is set to have a concrete impact in terms of incident visibility. It introduces a harmonised, comprehensive framework for digital operational resilience for EU financial institutions and also establishes a reporting regime for major Information and Communication Technology (ICT) incidents by EU financial institutions.

This paper aims to contribute to the evolving architecture for monitoring and assessing cyber and operational risk from a financial stability perspective. It builds on the framework introduced by ESMA in 2018, which recognises cyber threats as a distinct and evolving risk category requiring specific analytical focus.

It explores conceptual frameworks to examine how individual incidents can become systemic, by focusing on exposures to cyber threats, the propagation of the shock through the system, and their impact.

The paper also presents findings from a simulation analysis conducted on the EU repo market suggesting that operational disruptions at a few market participants can lead to temporary yet severe liquidity shortages at both the system and counterparty levels, with widespread network effects. These mechanisms can magnify the initial shock and contribute to broader financial instability.

While no incident has yet significantly impacted the financial system, the analysis illustrates how cyber shocks could evolve into more conventional risks, such as liquidity crises and market disruptions, and have systemic consequences.

By integrating conceptual modelling, stress-simulations, and systemic metrics, this paper exemplifies the type of analytical toolset envisioned in ESMA (2018) and underscores the value of these methodologies to better understand, assess and measure cyber risk.

Related reading

Brando, D., Kotidis, A., Kovner, A., Lee, M., Schreft, S., L. (2022), “Implications of Cyber Risk for Financial Stability”, FEDS Notes.

Bouveret, A. (2019), “Estimation of losses due to cyber risk for financial institutions”, Journal of Operational Risk, vol. 14, no. 2 (June), pp. 1-20.

Boston Consulting Group (BGC, 2019), “Global Wealth 2019: Reigniting Radical Growth”.

Center for Strategic and International Studies (2020), “The Hidden Costs of Cybercrime”.

Coste, C., Tcheng, C., Vansieleghem, I. (2021), “One size fits some: analysing profitability, capital and liquidity constraints of custodian banks through the lens of the SREP methodology”, ECB Occasional Paper Series, no. 256.

Duffie, D., Younger, J. (2019), “Cyber Runs”, Hutchins Center Unpublished Working Paper 51, Brookings Institution.

Embroker (2024), "How Much Does a Data Breach Cost in 2024?".

European Central Bank (ECB, 2024), “ECB concludes cyber resilience stress test”, Press release.

European Central Bank (ECB, 2025), “Cyber resilience stress testing from a macroprudential perspective”, ECB Macroprudential Bulletin, no. 27.

European Union Agency for Cybersecurity (ENISA, 2016), “The cost of incidents affecting CIIs”

European Union Agency for Cybersecurity (ENISA, 2024), “Enisa Threat Landscape 2024”

Eisenbach, T., M., Kovner, A., Lee, M., J. (2021), “Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis”, Federal Reserve Bank of New York Staff Reports, no. 90.

Joint Committee of the European Supervisory Authorities (ESA, 2024), “Draft Regulatory and Implementing Technical Standards on the content of the DORA major incidents reporting”, Final Report.

European Securities Market Authority (ESMA, 2021), “Guidelines”, Reporting under Articles 4 and 12 SFTR.

European Securities Market Authority (ESMA, 2024), “EU Securities Financing Transactions markets 2024”, ESMA Market Report.

European Securities Market Authority (ESMA, 2018), “Operational risk assessment – the ESMA approach”, ESMA Report on Trends, Risks and Vulnerabilities No. 1, 2018, pp. 68ff.

European Systemic Risk Board (ESRB, 2020), “Systemic cyber risk”, Tech. rep. European Systemic Risk Board.

European Systemic Risk Board (ESRB, 2022), “Mitigating systemic cyber risk”, Tech. rep. European Systemic Risk Board.

European Systemic Risk Board (ESRB, 2023), “Advancing macroprudential tools for cyber resilience”.

European Systemic Risk Board (ESRB, 2024), “Advancing macroprudential tools for cyber resilience – Operational policy tools”.

Financial Stability Board (FSB, 2018), “Cyber Lexicon”.

Financial Stability Board (FSB, 2020), “Effective Practices for Cyber Incident Response and Recovery”.

Financial Stability Board (FSB, 2021), “Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence”.

Financial Times (FT, 2024), “Ransomware attack on ICBC disrupts trades in US Treasury market”.

Fitch Ratings (FITCH, 2023), “Cyberattack at a US Subsidiary of ICBC Highlights Payment Interruption Risks”.

Healey, J., P. Mosser, K. Rosen, A. Wortman (2018), “The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability”, Project on Cyber Risk to Financial Stability, School of International and Public Affairs, Columbia University, New York.

ID Theft Resource Center (2020), “Data breach report”.

Iyer, R., Macchiavelli, M. (2017), "The Systemic Nature of Settlement Fails," FEDS Notes. Washington: Board of Governors of the Federal Reserve System, July 3, 2017.

Moody’s (2021), “Sunburst attack on public and private entities raises credit risks as extent of

breach unfolds”, March 2021.

International Capital Market Association (ICMA, 2023), “A Guide to Best Practice in the European Repo Market”, November 2023.

International Monetary Fund (IMF, 2024), “Global Financial Stability Report”, April 2024.

Kaffenberger, L., Kopp, E. (2019), “Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment”, Cyber Policy Initiative Working Paper Series, “Cybersecurity and the Financial System”, No. 4, Carnegie Endowment for International Peace, Washington, DC.

Kashyap, A.K., Wetherilt, A. (2019), “Some principles for regulating cyber risk”, AEA Pap. Proc., 109, pp. 482-487.

Reuters (2024), “Explainer: What is Lockbit? The digital gang shutdown after a cybercrime spree”.

Reuters (2023a), “Yellen: no impact on US Treasury market from ICBC hack”.

Reuters (2023b), “Inside Wall Street's scramble after ICBC hack”.

Ross, G. (2020), “The making of a cyber crash: a conceptual model for systemic risk in the financial sector”, Occasional Paper Series, No. 16, May, European Systemic Risk Board.

Statista (2022), “Cybercrime Expected to Skyrocket in Coming Years”.

The Banker (2023), “The significance of the ICBC FS hack on the US Treasury market”.