BANCO DE ESPAÑA
Eurosistema

12.04.2024

Cyber risk and its implications for financial stability*

Punto de Encuentro Financiero FINANZA/Elkargi
Bilbao

Pablo Hernández de Cos
Governor

* English translation from the original in Spanish.

Ladies and gentlemen, good morning. Let me begin by thanking Elkargi for organising this event and for offering me the opportunity to take part.

On this occasion I would like to share with you some reflections on cyber risk[1] and its implications for financial stability. The relentless digitalisation of the economy and of society at large has made it a priority for us all, but especially for the financial sector and its supervisory and regulatory authorities.

The growing digitalisation of the banking business …

The financial sector is extensively digitalised. Banks depend on technology not only as a fundamental support for business processes, but also as a differential and competitive factor.

In recent years, digitalisation has accelerated, both to improve the efficiency of banks' internal processes and to offer their customers flexible, personalised and immediate services, accessible anywhere and via a range of devices.

The COVID-19 pandemic and the emergence of new competitors, such as bigtechs or fintechs, have reinforced these developments.

… has increased the exposure of financial institutions and their customers to cyber risk …

This digitalisation process has intensified the financial sector's exposure to cyber risks. Similarly, by broadening access to remote financial services, it has increased customers' exposure to cyber attacks and digital fraud.

The number of cyber incidents – especially of malicious cyber attacks[2] – has grown continuously in recent years, with the financial industry among the sectors most affected.[3] Moreover, not only are cyber attacks on the rise, but they are also more sophisticated and have a larger potential impact,[4] regardless of whether they are strictly economically or geopolitically motivated. In particular, cyber attacks have become more frequent since Russia invaded Ukraine.

[1] Cyber risk is understood as the combination of the likelihood of cyber incidents occurring and their impact. In its Cyber Lexicon, the Financial Stability Board (FSB) defines cyber incidents as events, whether or not malicious, that compromise the confidentiality, integrity or availability of information or interconnected information systems.

[2] Cyber incidents include those caused by natural disasters, human error or accidental system failures. Indeed, non-malicious cyber incidents are the most frequent, although the impact of cyber attacks, despite being less frequent, is usually greater.

[3] In 2023 the National Cryptology Centre registered 107,777 cyber incidents, compared with 42,997 in 2019. The recently published 2023 National Security Report (*Informe Annual de Seguridad Nacional 2023*) cites the financial sector, along with energy, ICT and transport, as those with the highest volume of cyber incidents in recent years.

[4] We are seeing cyberattacks in the form of transfer fraud, cryptocurrency theft and ransomware (where the attackers demand a ransom in exchange for returning and not disclosing their victims' encrypted information).

By type of cyber incident, cases of fraud that use social engineering, such as phishing,[5] smishing[6] and vishing,[7] have risen sharply, along with website and mobile app impersonation, among others.

The losses associated with cyber incidents are also significant. For instance, data leaks – one type of cyber attack that has become increasingly common – cost firms $4.45 million on average worldwide in 2023. In the financial sector, data leaks were not only more frequent, but the average cost was also higher ($5.9 million in 2023).

Moreover, the possibility of transferring this risk is limited. The financial cover offered by cyber incident insurance policies does not usually extend to all the effects of such incidents.[8] In addition, the terms and conditions of these policies have tightened recently worldwide.

… and can affect financial stability

Financial institutions considered individually have extremely complex technological environments, where old software coexists with other programs that depend on newer technology, the result not only of transformation processes, but also, in some cases, of successive mergers and acquisitions. This complexity makes maintaining an adequate control environment challenging for banks. It also makes them more vulnerable to system failures and cyber attacks.

The financial sector as a whole is also a highly complex ecosystem, consisting of many participants who are very closely interconnected and interdependent. And we are not just talking about financial interconnections: there are also operational interconnections between industry participants, through market infrastructures, common service providers and even the provision of services between financial institutions.

In addition to these traditional interconnections, there are also the new financial service providers to be considered, as well as the growing dependence on technology providers. In many cases this dependence is highly concentrated on a relatively small number of providers. This is true particularly for cloud service providers, some of which constitute single points of failure. In consequence, cyber incidents affecting these providers – even unintentional ones – can impact the entire sector and thus become systemic.[9]

[5] Phishing attacks are those in which the attacker fraudulently tries to obtain confidential information (passwords, bank details, etc.) from legitimate users by supplanting the digital identity of a trusted bank.

[6] Smishing is a technique that consists of a cybercriminal sending an SMS to a user, pretending to be a legitimate bank, with the aim of stealing private information or charging their account.

[7] Vishing is a type of social engineering scam over the telephone in which the caller supplants the identity of a trusted company, organisation or person in order to obtain personal and sensitive information from the victim.

[8] For example, compensation payments cannot cover some of the most important impacts of a ransomware attack, such as the shutdown of a bank's infected systems, which must be resolved as swiftly as possible.

[9] For instance, a large-scale attack on a great number of banks or against a critical provider, or failures in software commonly used in the sector, would be scenarios with a potential systemic effect.

For this reason, macroprudential authorities in different jurisdictions – for instance, the European Systemic Risk Board (ESRB) – include cyber risk among the main sources of systemic risk in the world today.[10]

From cyber risk to cyber resilience: towards a holistic approach

Given all the above, it is not surprising that financial institutions and prudential authorities alike are prioritising the implications of cyber risk and the possible mitigating measures.

In this respect, as we move towards a fully digital world in which cyber threats are becoming increasingly frequent and sophisticated, a paradigm shift becomes essential. As does the need to accept that, despite all our preventive efforts, at some point there will be a cyber incident that has an impact.

The idea of cyber resilience stems from the concept of cyber security and is understood as the ability of an organisation to continue pursuing its business, anticipating and adapting to cyber threats and other key changes in its environment, withstanding, containing and quickly recovering from any cyber incidents.[11]

In turn, cyber resilience can be seen as an extension of the concept of operational resilience, understood as an organisation's ability to maintain its critical operations in adverse circumstances.[12]

It is, therefore, a holistic approach, which is not exclusively focused on managing technology but attaches equal importance to an organisation's people and processes and ties in with more traditional concepts such as business continuity.

Banks are moving towards this holistic approach. In addition to continuously improving technical measures, they are making important efforts to educate and raise awareness about cyber security among their staff, seeking to ensure that they do not become access vectors for attackers.

In the same vein, in recent years banks' senior management have accumulated more knowledge and become more aware of cyber risk, while cyber risk management and audit functions have been strengthened. Banks are also striving to raise awareness about the importance of cybersecurity among their customers.

The necessary regulatory and supervisory response

A broad prudential supervisory and regulatory response is being implemented, globally, across Europe and in Spain, both at microprudential and macroprudential level. Globally, in 2021, the Basel Committee on Banking Supervision (BCBS) approved the Principles for

[10] See, for example, ESRB. (2020). *Systemic cyber risk*.

[11] See the FSB's *Cyber Lexicon*.

[12] BCBS. *Principles for Operational Resilience*.

Operational Resilience, which establish that banks should assume as a working hypothesis that disruptions will occur and should define their tolerance for disruption. The principles encompass both preventive and pre-emptive measures as well as those aimed at response and recovery when disruption to critical services occurs.[13]

Noteworthy in the European Union is the Digital Operational Resilience Act (DORA), which seeks to mitigate the risks associated with digitalisation and bolster sector-wide resilience by means of:

- Information and communication technology (ICT) risk management and third-party risk management requirements for all financial institutions.

- The obligation to report ICT-related incidents to supervisors so that potential adverse events that may require some form of intervention by the authorities can be detected as early as possible.

- System resilience testing. The most advanced tests consist of simulating cyber attacks, using intelligence on the most likely attackers and their modus operandi. The aim is to assess financial institutions' technical, human and organisational capacities to detect and respond to an attack.

On the microprudential supervision front, European banking sector financial authorities have incorporated cyber risk as one of their supervisory priorities, as a result of which all ongoing monitoring and on-site inspections of banks and horizontal activities targeting cyber risk are being strengthened.

To this end, they have boosted their specialised resources and have established methodologies and working procedures adapted to cyber risk's specific features. The Single Supervisory Mechanism will conduct a cyber resilience stress test in 2024.

In 2017 the ESRB set up the European Systemic Cyber Group, a dedicated task force to study cyber risk's potential impact on financial stability. The different analyses performed show:

- The usefulness of working on cyber resilience stress test scenarios at a systemic level.[14]

- The need for systemic cyber incident response plans and for them to be regularly reviewed and tested.

[13] These principles cover: governance; operational risk management; business continuity planning and testing; mapping interconnections and interdependencies; third-party dependency management; incident management; and ICT, including cyber security.

[14] DORA also encourages authorities to organise crisis management and contingency exercises involving cyber attack scenarios, with a view to gradually enabling an effective coordinated response at European Union level.

- The desirability of identifying the circumstances in which a systemic crisis may be triggered and establishing thresholds that enable a rapid response and preventive mitigation measures (systemic impact tolerance objectives (SITOs)).[15]

- The need to create a pan-European systemic cyber incident coordination framework that fills the current gaps.

Meanwhile, from this systemic standpoint, DORA encourages information sharing between institutions and establishes arrangements for cooperation between financial and non-financial sector authorities. It also tasks the European supervisory authorities with assessing the feasibility of a single EU Hub for major ICT-related incident reporting for all European financial institutions and establishes an oversight framework for those ICT providers that are critical to the European financial sector.

Macroprudential tools to manage cyber risk: from financial capital to technological capital

In parallel, a discussion is under way on the most appropriate tools to mitigate cyber risks.

Prudential capital's role in particular has been analysed. In this case, the survival of a bank affected by a ransomware attack that encrypts all of its critical systems would depend on whether or not it has the technical measures in place to allow it to recover. Capital would therefore not be the backbone of its resilience.

However, aside from higher solvency potentially meaning it is easier to fund the means required to recover from a cyber incident, the potential disruptive consequences for the financial system as a whole may sometimes warrant the release of macroprudential capital buffers so that banks can continue supplying credit to the economy. For example, the systemic risk buffer could be used to distinguish between banks based on their technological systemicity. This could help limit the occurrence of systemic events and subsequent spillover effects.

The materialisation of cyber incidents with a significant financial impact may require financial instruments for crisis management to be used and even new ones to be developed. A bank could see its operations curtailed as a result of a cyber incident, leading to liquidity problems. Central banks providing liquidity to solvent banks whose liquidity has dried up because of a cyber incident could allow such banks to continue their activity, helping to mitigate the potential risk to financial stability and allowing them to continue providing services to the economy.

In a similar vein, resolution and recovery plans, while not specifically designed for such situations, may be adapted to ensure the continuity of the critical functions of the banks potentially affected by the incident.

In any event, the cyber resilience afforded by a certain amount of capital could probably be achieved more efficiently and effectively by building up technological resources (software,

[15] A SITO could be defined for a specific economic function based on the number of transactions affected, their value in euro, the duration of the cyber incident and the number of banks and jurisdictions affected.

hardware, know-how, specialists, etc.) to render cyber incidents less likely and lessen their financial impact. For example:

- The introduction of circuit-breakers that suspend processes in the event of simultaneous technological and financial crises, limiting their spillover effects.

- Collective support arrangements whereby banks share technological capital, enabling system-wide collaboration between banks to get processes back on track should one fail or, similarly, providing access to data compromised in an isolated cyber attack. Specifically, data vaulting strategies include offline and offsite storage of the information that a bank needs to operate its critical services. The most advanced example is Sheltered Harbor, which involves and is supported by the main US banking associations. Participating banks send their encrypted data in an agreed format to shared facilities so that their data can be recovered and processed on a recovery platform.

Future outlook: artificial intelligence and quantum computing

The possibilities provided by new technologies will afford new opportunities to defenders and attackers alike.

In the case of artificial intelligence (AI), content generation capacities will facilitate identity theft and make social engineering attacks much more credible. AI can also help create malware and optimise attacks.

Conversely, it may enable banks to identify cyber threats early through pattern recognition based on large volumes of near real-time data. It may also enable the response to be partially automated, thus complementing the work of analysts and substantially shortening response times.

Meanwhile, it is estimated that quantum computing could mean that many of the current encryption systems will be breached in the medium term. This will affect both the confidentiality and the integrity of the encrypted data, potentially leading to the manipulation of legal history via tampering with signed documents or the creation of validly signed falsified documents.

However, work is already under way to create quantum-safe cryptographic algorithms and to plan the migration of hardware, software and services using potentially vulnerable cryptography to such algorithms.

Conclusions

In sum, although some studies suggest that the financial industry is one of the key sectors best prepared against cyber risk, in part because of its high degree of regulation and supervision, the acceleration of digitalisation, the development of new technologies, the sector's systemic nature and the complexity and growth of technology risk all mean that

cyber risk should remain a key focal point over the coming years, and that recent efforts should even be stepped up.

This adaptation will require organisations to recruit the necessary technical profiles. As a result, attracting and retaining talent will remain a challenge for the sector and for the authorities.

Sharing information on cyber threats and cyber incidents will also be key to improving collective defence capabilities. In this respect, the central role of the authorities, which under DORA will receive reports on cyber incidents from banks, will allow them to give the sector useful feedback.

Similarly, cyber resilience stress tests and sectoral crisis management exercises, involving critical providers and other sectors with which there are operational interdependencies, will be essential over the coming years.

In addition, further progress is needed on the quantification and understanding of cyber risks for financial stability and the potential role of macroprudential policies in mitigating them.