Special Feature

CYBER RISK

Cyber risk can be defined as the combination of the probability of cyber incidents ocurring and their impact,[1] where cyber incident means a cyber event that adversely affects the confidentiality, integrity and availability of information or an information system, whether resulting from malicious activity or not. These events are in fact becoming increasingly relevant to the financial system as a whole and to other productive sectors as the digitalisation of the economy and society progresses.[2] Moreover, financial and technological interconnectedness means that cyber incidents can spread rapidly across banks, non-banks and financial market infrastructures with potential financial stability implications. Reliance on critical services provided by third parties entails new vulnerabilities and concentration risks within the financial system.

Against this background, prudential regulators and supervisors are paying the utmost attention to these new risks and promoting initiatives to make financial institutions more resilient to them, i.e. to strengthen their cyber resilience. The authorities' initiatives increase the already high incentives for financial institutions to invest in technological resources, in order to protect not only their data but also the integrity of the provision of services to their customers.

The European authorities' initiatives include the recent approval of the Digital Operational Resilience Act (DORA),[3] the NIS 2 Directive on cyber security,[4] the ongoing work to implement the European Systemic Risk Board (ESRB) recommendation on coordination in the event of systemic cyber incidents, and supervisory stress testing of banks' resilience to cyber attacks by the Single Supervisory Mechanism in 2024.

The rest of this special feature is structured as follows. Section SF.1 analyses the concepts of cyber risk and cyber resilience in the context of the digitalisation of the financial system. Section SF.2 describes the growing frequency and impact of cyber risk. Both sections draw on publicly available cyber risk data, subject to multiple limitations. Section SF.3 sets out the various initiatives of financial institutions themselves, micro- and macroprudential authorities and other organisations to strengthen cyber resilience. Section SF.4 concludes with possible outlooks for cyber risk, for example in relation to the impact of artificial intelligence, and for institutions' and authorities' tools to mitigate them, which will have to focus on the provision of adequate technological resources, on top of the financial resources used to absorb operational losses.

1 See the Financial Stability Board's (FSB) Cyber-Lexicon for definitions of relevant cyber risk terms.

2 See the European Commission report of 24 January 2024.

3 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

4 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

SF.1 Cyber risk and the financial system

SF.1.1 The financial system as an ecosystem

The financial system is highly complex, with many highly interconnected and interdependent participants. This system comprises market infrastructures, the various types of financial institutions (banks and non-banks) and their main technology service providers, as well as all of their supervisory authorities. Financial institutions have both direct interconnections through their assets and liabilities and indirect ones, since they invest and raise funds using those same types of instruments (see Section 2 of Chapter 2 of this *Financial Stability Report).* In addition, there are numerous operational interconnections between participants in the sector, through market infrastructures, common service providers and even the provision of services between financial institutions.

Because of these interconnections between institutions and other characteristics of the financial system, cyber risk can threaten financial stability.[5] Thus, cyber incidents may not only affect each individual participant, but also spread and magnify, and have systemic implications for the sector as a whole. In addition to interconnectedness, other relevant features of the financial system for assessing cyber risk include its strong reliance on technology, its appeal to attackers with different motivations (e.g. financial and political) and a high sensitivity to a loss of confidence among its participants.[6]

Financial institutions complement their technological capabilities through various relationships with other agents. These include procurement of services from suppliers, participation in consortia, investments in start-ups or purchases of products from third parties.

In many cases, the supply of technology services is highly concentrated among a relatively small number of providers, particularly in the area of cloud computing.[7] In fact, some of these providers have come to form the backbone of the financial system, at a level comparable to market infrastructures. In cloud computing, for example, three companies account for more than 60% of the market share[8] and their simultaneous failure would have an adverse systemic impact on operations. They are therefore single points of failure, since the incidents affecting them, including unintentional ones, have an impact on the sector as a whole. Moreover, many of these suppliers also provide their services to companies in other sectors, making them potentially critical to the economy of entire countries or even groups of countries.

---

5 F. J. Herrera Luque, J. Munera López and P. Williams. (2021). "Cyber risk as a threat to financial stability", *Financial Stability Review – Banco de España,* 40.

6 See the ESRB report *Systemic cyber risk* of February 2020.

7 The European Banking Authority (EBA) defines cloud computing as a model for enabling ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

8 Ting Yang Koh and Jermy Prenio. (2023). *Managing cloud risk - some considerations for the oversight of critical cloud service providers in the financial sector.* FSI Insights on policy implementation No 53.

Identifying all of the sector's interdependencies is a complex challenge. Traditional financial institutions are connected with each other and with market infrastructures, there are new players offering financial services (e.g. FinTech)[9] and there is a growing reliance on direct technology providers. But there are also other dependencies on third parties that have not been properly identified, created by successive outsourcing along the technological product and services procurement chains, over which financial institutions have little or no control. This has led initiatives such as the FSB's toolkit[10] for enhancing third-party risk management or the European Union's DORA Regulation, analysed in more detail in Section SF.3, to focus on these dependencies.

SF.1.2 Digital transformation and cyber risk exposure

The financial system is highly digitalised and financial institutions rely on technology not only to do business, but as a differential and competitive factor. In recent years the digital transformation process has accelerated enormously,[11] in terms of both improving the efficiency of financial institutions' internal processes and providing their customers with flexible, personalised and immediately accessible services, from anywhere and on different types of devices.[12] This has been reinforced by the emergence of new competitors for traditional financial institutions, such as BigTech[13] and FinTech firms, which can provide highly attractive solutions in a very agile and innovative way.

The high level of digitalisation in the financial system increases its exposure to cyber risk. Most financial institutions have extraordinarily complex technological environments, where legacy applications coexist with others based on more innovative technologies, as a result not only of transformation processes but also in some cases of successive mergers and acquisitions.[14] This complexity makes it difficult for institutions to maintain an adequate control environment and, therefore, makes them more vulnerable to both system failures and cyber attacks.

Against this background, the COVID-19 pandemic has acted as an accelerator, changing the way financial institutions operate and their relationship with customers. For example, teleworking, which remains stable at a higher level than before the pandemic, poses additional risks to institutions and their staff, including those arising from accessing corporate systems from personal devices and home networks and handling confidential data in employees'

9 The FSB defines FinTech as technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services. The companies using these technological innovations are commonly referred to with the same term.

10 See the FSB report *Enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities* of 4 December 2023.

11 According to the FUNCAS – KPMG Financial Digitalisation Observatory report, *La digitalización como eje de transformación bancaria* (only available in Spanish), the penetration of digital banking in Spain increased from 54.9% in 2019 to 69.6% in 2022, almost 10 percentage points higher than the European average for 2022 (59.7%). The report also highlights that advancing the digital transformation was a strategic priority for 58% of institutions in 2022, outranking mitigating the effects of inflation, which was a priority for 53%.

12 José Ramón Martínez Resano. (2022). *Regulating for Competition with Bigtechs: Banking-As-A-Service and 'Beyond Banking'*.

13 The FSB defines BigTechs as large technology companies with extensive customer networks.

14 See "Changes in the main Spanish banking groups (2009-2021)", Banco de España.

homes. Customers' electronic access to various financial services was boosted by restrictions on mobility during the initial stages of the pandemic, and part of this momentum continued thereafter as social relations returned to normal.

The greater availability of remote financial services has increased the exposure of the customers using these services to cyber attacks and fraud. There has been a very significant increase in social engineering fraud such as phishing,[15] smishing[16] and vishing,[17] as well as scam websites and mobile applications, among others. Despite institutions' efforts to improve customer cyber security education, some customers continue to be highly vulnerable, particularly those who had never used digital channels prior to the pandemic.

Although some studies suggest that the financial sector is one of the critical sectors best prepared for cyber risk, there is some heterogeneity at the level of individual institutions. While the sector's better relative position is partly due to its high level of regulation and supervision, in some cases the security measures and controls implemented by institutions (particularly smaller ones) still need to be improved to adequately manage cyber risk.

SF.1.3 Non-malicious events and cyber attacks

Cyber incidents are not limited to cyber attacks. The definition of cyber incident in the FSB's Cyber Lexicon (see footnote 1) refers to events whether resulting from malicious activity (caused by cyber attacks) or not. The latter, which include events caused by natural disasters (e.g. earthquakes), human error or accidental system failures, may also affect the ability of institutions and the sector to continue operating normally. Accordingly, resilience to these cyber incidents is equally important.

The different types of cyber incidents vary in frequency and impact. Looking at the main causes of cyber incidents reported annually to the European Union Agency for Cybersecurity (ENISA) across all sectors, non-malicious incidents, such as system failures or human error, are the most common (see Chart SF.1).[18] Despite their prevalence, in most cases these incidents do not have a significant impact, either individually or systemically. Malicious incidents, which account for around 22% of the total, have a greater impact.

The very nature of malicious cyber incidents and their intentionality explain their greater impact despite their lower frequency. In most cases, these are attacks designed to have the

15 Phishing attacks are those where the attacker tries to fraudulently obtain confidential information (passwords, bank details, etc.) from legitimate users, by posing as a trustworthy institution.

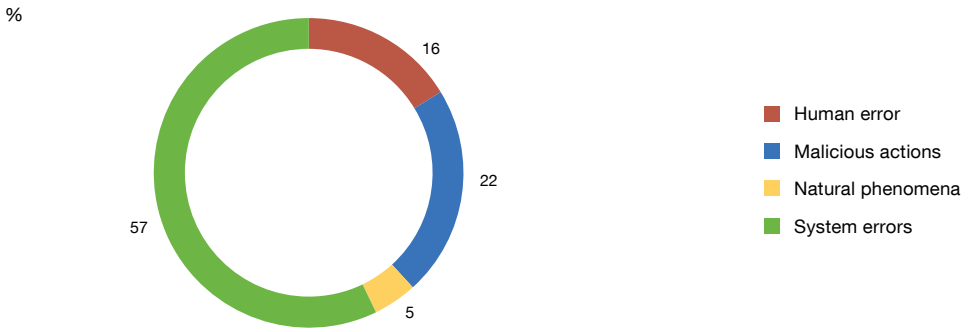
16 Smishing is the practice of sending text messages purporting to be from a legitimate institution with the aim of stealing users' private information or money.

17 Vishing is a type of social engineering scam via telephone, where the identity of a trustworthy firm, organisation or person is supplanted through a call, with the aim of obtaining the victim's personal and sensitive information.

18 All the charts in this special feature use the best possible approximation based on publicly available data to illustrate various relevant stylised facts relating to cyber risk. These approximations have important limitations in terms of the quantity and quality of the available data. Supervisors have far superior confidential data. The high priority of cyber risk on the regulatory and supervisory agenda suggests that more aggregate data will become available in the future.

Chart SF.1
Despite their stronger impacts, malicious cyber incidents account for a limited percentage of total reported cyber incidents

SF.1.a Causes of the cyber incidents reported to ENISA in Europe between 2013 and 2023



SOURCES: ENISA, Cybersecurity Incident Reporting and Analysis System.

greatest possible impact on their victims, for example by paralysing their operations or stealing confidential data. In addition to this, attackers may try to increase their scope and impact: from a single user to a wider group of one or more institutions. The long-term effects of these incidents, such as reputational damage, also contribute to their greater impact.

SF.1.4 From cyber security to cyber resilience

The concept of cyber security has a well-defined scope. The FSB's Cyber Lexicon defines cyber security as the preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. It therefore primarily concerns prevention and protection. However, as we move towards a fully digital world where cyber threats are becoming more frequent and sophisticated, a paradigm shift is required in which we must assume that a major cyber incident will occur at some point in time.

The concept of cyber resilience builds on that of cyber security. The FSB's Cyber Lexicon defines cyber resilience as an organisation's ability to continue to perform its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

Thus, cyber resilience relates to the broader concept of operational resilience. The Basel Committee on Banking Supervision (BCBS) defined operational resilience in its Principles for Operational Resilience[19] as the ability of a bank to deliver critical operations through disruption. This definition can be applied not only to banks, but also to all kinds of private firms and public institutions inside and outside the financial system. This is a more holistic approach that does

19 See the BCBS report *Principles for Operational Resilience* of March 2021.

not focus solely on the technology itself, but gives the same importance to people and processes in organisations and links up with existing disciplines, such as business continuity.

SF.1.5 The relationship between cyber risk and economic and financial risks

Individual level

Cyber risk events can have a significant individual impact at the operational level, but also beyond. In a highly digitalised environment, technology is a factor that affects all areas of business activity. Cyber risk can therefore have an impact on other risks, such as legal, reputational or traditional financial risks.

Cyber incidents can have a potentially serious impact on an institution's reputation. Unavailability of services or breaches of confidentiality or of the integrity of information held by financial institutions, whether due to malicious or accidental events, may have an impact on the confidence of customers and the market in general. These reputational impacts may be exacerbated if the public disclosure of the cyber incidents is not properly managed.

Systemic level

The interaction between cyber risk and other risks (such as financial risk) increases at the systemic level. In addition to the implications of cyber risk at individual level, at systemic level the high interconnectedness and interdependence between financial institutions must also be taken into account. Thus, the impact of a cyber incident in one institution may spread to others, adding to the operational, financial and reputational impact, and potentially eroding confidence in the sector, a crucial element that could exponentially increase the impact at the systemic level. Other scenarios with a potential systemic effect include, for example, a massive attack against a large number of institutions or a critical provider, or failures of software commonly used in the sector.

The systemic financial stability implications of cyber risk are being analysed by the macroprudential authorities. For example, over the last few years the ESRB has been studying the impact of cyber risk on financial stability,[20] the potential channels of contagion through which the impact of a cyber incident may threaten financial stability[21] and possible measures to mitigate it.[22]

The materialisation of risks linked to the credit or business cycle does not necessarily reduce the probability of cyber incidents. On the contrary, a recession could increase incentives for financially motivated malicious attacks, as it would reduce technological agents'

20 See the ESRB report *Systemic cyber risk* of 19 February 2020.

21 ESRB. (2020). "The making of a cyber crash: a conceptual model for systemic risk in the financial sector", ESRB Occasional Paper Series, 16.

22 See the ESRB report *Mitigating systemic cyber risk* of 27 January 2022.

ability to generate legitimate income and institutions' capacity to invest in cyber resilience. While more research is needed on this issue, should cyber risk remain neutral or intensify with the economic/financial cycle, it would be necessary to set aside dedicated resources to absorb it. These resources would have to be specifically categorised as such and would be adapted to the technological nature of these risks.

SF.2 The impact of cyber risk

SF.2.1 Main cyber threats

There are different types of cyber threat actors, varying in their motivations, the sophistication of attacks and the impact they have. Amateur attackers[23] and activists[24] usually seek publicity and tend to carry out less sophisticated and low or moderate impact attacks. So-called insiders[25] are often motivated by revenge or hired as spies by others; their knowledge of the company and easy access to it make them potentially dangerous, even if they do not always have strong technical skills. However, there are other types of attackers, that may be geopolitically or purely economically motivated, with highly sophisticated technical capabilities, that can cause very serious damage.

Cyber attacks attributed to organised crime, for financial gain, are on the rise worldwide. This is resulting in growing costs (see Chart SF.2). The existing legislation is essentially limited to a physical environment with well-defined sovereign jurisdictions, making it difficult to apply to the digital world. There are also huge differences between jurisdictions, and global agreements to pursue this type of crime are virtually non-existent. This situation, combined with the difficulty of tracing crimes to their perpetrators, makes cyber attacks a criminal offence with low risk for the offender and high costs for the institutions and individuals affected.

There has also been an increase in geopolitically motivated cyber attacks. The targets and techniques used vary from one another. For example, in the context of the conflict between Russia and Ukraine, supporters of both sides have launched numerous denial of service attacks[26] against public administrations and companies in countries supporting the other side, in order to create instability and hinder all types of activity in those countries, including financial activity. In other cases, State-backed groups seek financial gain from their attacks,[27] by making fraudulent transfers,[28] stealing cryptocurrencies[29] or demanding ransom in exchange for returning information encrypted by the attackers to their victims and not disseminating it

23 Also known as script kiddies.

24 They are often called hacktivists.

25 In this context, insiders are employees acting for malicious purposes against their companies.

26 A denial of service attack consists of flooding a website with requests until it becomes inoperable.

27 United Nations Security Council report (2019).

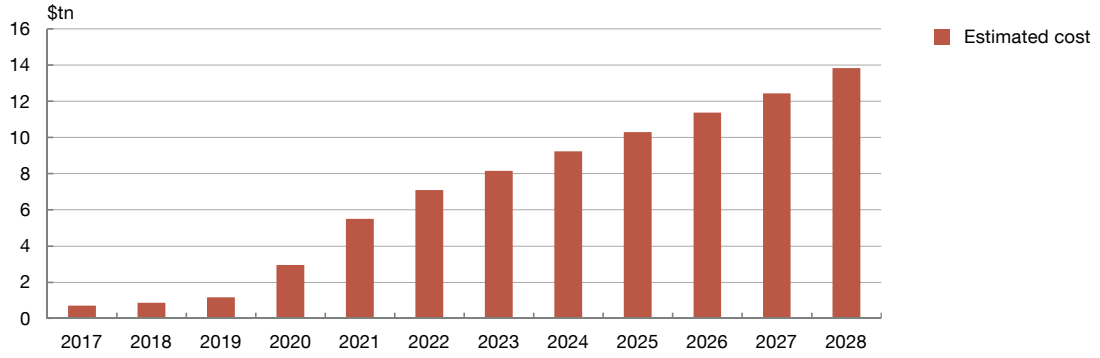
28 For example, the attack on the central bank of Bangladesh in 2016 in which fraudulent transfers were made via the SWIFT network totalling over $80 million. See news article.

29 For example, it is estimated that the Lazarus group, associated with the government of North Korea, was responsible for 20% of crypto-asset thefts in 2023 (over $300 million). See news article.

Chart SF.2

The estimated global cost of cyber crime has increased almost tenfold in the last five years and this growing trend is expected to continue

SF.2.a Estimated global cost of cyber crime



SOURCE: Statista, Statista Technology Market Insights.

(ransomware).[30] Data theft is another channel used by attackers to obtain financing and State-financed cyber attacks seeking to obtain sensitive information that may be economically or politically useful are becoming increasingly frequent.

The number and sophistication of cyber attacks against financial system providers, carried out by attackers with high technical skills, has grown. Some attacks are limited to exploiting existing vulnerabilities in these providers' hardware or software products.[31] Other more sophisticated attacks alter these products to introduce weaknesses that can then be exploited.[32] Despite the time and resources needed to prepare and carry out such an operation, this can allow the attackers to infiltrate thousands of organisations and firms through a single point of entry, thereby significantly multiplying the attack's effectiveness and efficiency.

SF.2.2 Cyber incidents and losses

Cyber incident volumes

The number of cyber incidents has risen steadily around the world in recent years, with a significant increase in malicious incidents following the COVID-19 pandemic. As expected, the increased use of digital technologies by firms, individuals and public

30 Ransomware is a type of malicious software that restricts access to certain parts or files of the infected operating system and then demands a ransom, often in cryptocurrency, to remove the restriction.

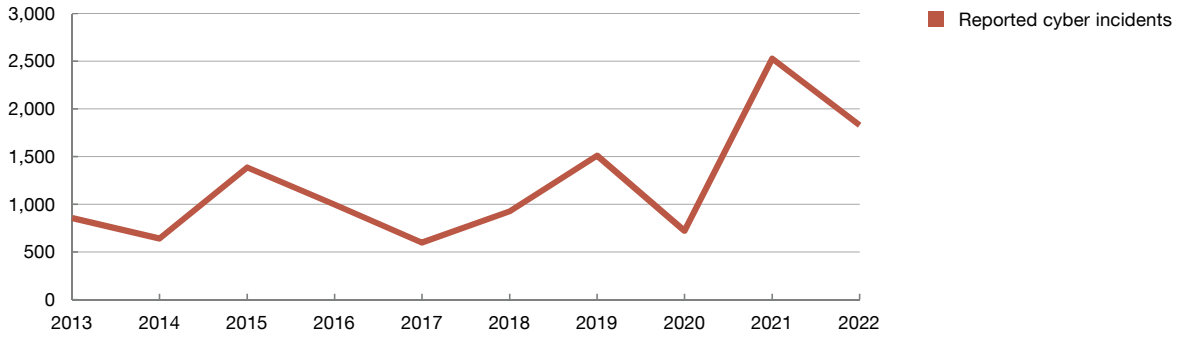
31 One of the many examples that can be cited is the exploitation of a vulnerability in the commercial file transfer software MOVEit by the Cl0p ransomware group, which affected thousands of organisations worldwide in 2023. See news article.

32 SolarWinds is the prime example of this. In December 2020 it was discovered that software distributed by this company had been modified by a group of cyber attackers so that it would grant them access to all of the software's users. Among the thousands of affected users were US federal agencies as well as NATO, the European Parliament, companies such as Microsoft, and others. See news article.

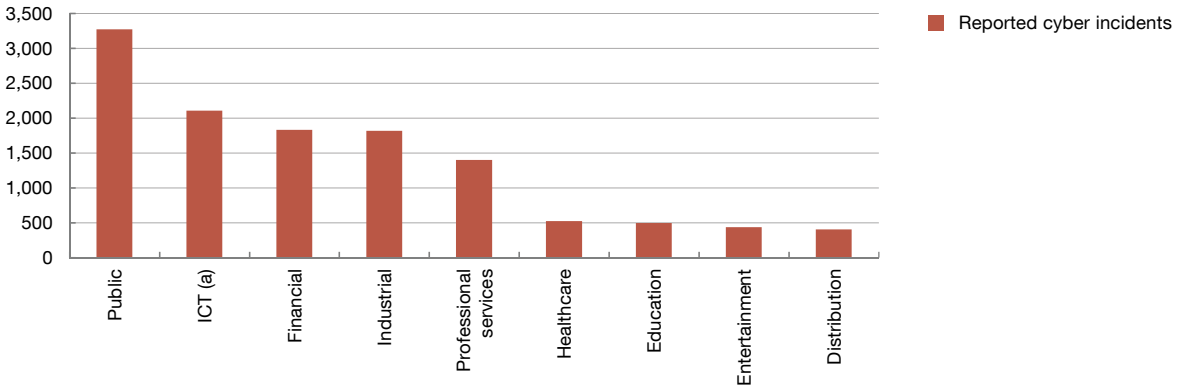
Chart SF.3

The financial sector continues to be one of the sectors with the highest number of cyber incidents worldwide. The annual number of cyber incidents reported in the financial sector has been growing steadily, doubling between 2018 and 2022

SF.3.a Global number of cyber incidents in the financial sector



SF.3.b Global number of cyber incidents in 2022, by sector



SOURCE: Verizon, *Data Breach Investigations Report 2023*

a Information and communication technologies.

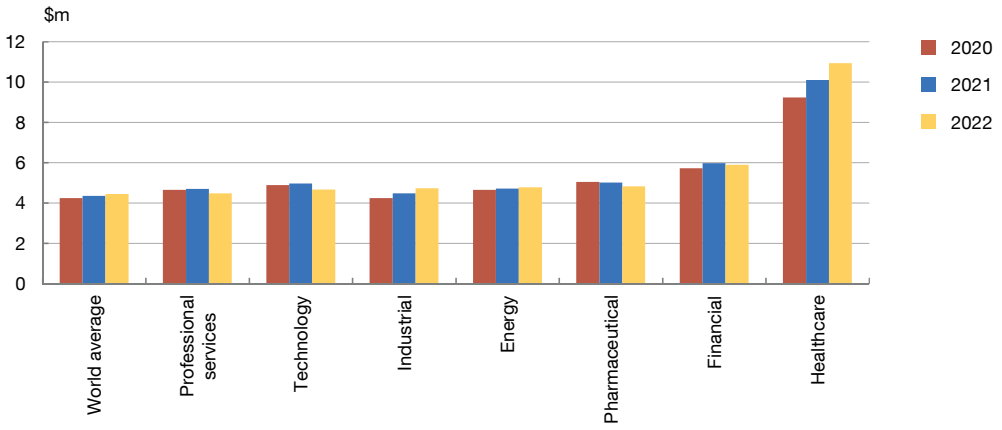
bodies has led to a steady rise in cyber incidents. For example, the sharp increase in the use of technology after the outbreak of the COVID-19 pandemic led to a significant overall increase in the number of cyber incidents reported in the financial system (see Chart SF.3.a). While the increase slowed after the worst of the pandemic, the upward trend is expected to continue.

The financial system is one of the most attacked sectors. This high relative prevalence of cyber incidents in the financial system (see Chart SF.3.b) persists, despite the fact that other sectors may occasionally be targeted. For example, the health sector was among the hardest hit during the COVID-19 pandemic and public administrations were the main target during the geopolitical tensions in 2022 (see Chart SF.3.b).

Chart SF.4

The global average cost of cyber incidents involving data breaches for the financial sector is second only to that for the healthcare sector

SF.4.a Average cost of a cyber incident involving data breaches, by sector



SOURCE: IBM, Ponemon Institute, *Cost of a Data Breach Report 2023*.

Losses

Losses from cyber incidents may vary considerably depending on different factors. As seen above, malicious cyber incidents typically result in higher losses for institutions due to their potential for greater impact. Data breaches, one of the most common cyber attacks, are also one of the costliest for institutions. The average cost of this type of incident is increasing globally each year, reaching $4.45 million in 2023.[33] In addition to being the one of the most targeted, the financial system is also one of the sectors with the highest average cost of data breach cyber incidents ($5.9 million in 2022) (see Chart SF.4).

Cyber insurance as a partial mitigant

The strategy of transferring risk has a limited scope in the case of cyber risk. Insurance against cyber risk, also known as cyber insurance, has a limited effect, as the financial coverage it provides may not be sufficient to mitigate the impact of a cyber incident. For example, monetary compensation cannot cover some of the most important impacts of a ransomware attack, such as the shutdown of an institution's infected systems, which must be resolved as quickly as possible.

Moreover, global cyber insurance terms and conditions have tightened. The insurance sector started to cover cyber risk without historical information or sufficient knowledge to correctly estimate premia. This was compounded by the significant increase in the frequency

33 See the IBM report *Cost of a Data Breach Report 2023*.

and impact of cyber incidents, leading to a rise in reported cyber insurance claims, which, for example, quadrupled in Spain between 2017 and 2020.[34] This increase, coupled with the low premia, had a negative impact on the profitability of this type of insurance policies. In recent years, insurance companies have responded by tightening renewal terms and conditions, increasing insurance premia and adding special clauses to exclude circumstances such as ransomware and wars.

SF.3 Managing cyber risk in order to strengthen individual and systemic resilience

SF.3.1 Good practices, regulation and supervision

Discussions on cyber risk in the financial system are high on the agenda of many international organisations. As economic activity has become increasingly digitalised and exposure to cyber risk has grown, these organisations have issued best practices, reports and tools. Among the most important in recent years are the FSB's Cyber Lexicon, mentioned above, and its effective practices for responding to and recovering from cyber incidents.[35] The FSB is also working on a common format for its reporting.[36]

The Basel Committee on Banking Supervision issued a noteworthy publication in this area: the Principles for Operational Resilience.[37] These aim to strengthen banks' capacity to withstand the impact of operational events that may disrupt their critical services. The Committee declared that banks should operate under the assumption that such events will occur and define their level of 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. They address (i) governance, (ii) operational risk management and ongoing identification of threats, (iii) identification of interconnections and interdependencies, (iv) management of third parties, (v) business continuity, (vi) incident management and (vii) technology management, including cyber security. Since their publication, jurisdictions have worked to incorporate these principles into their regulatory framework and supervisory practice, and banks are making progress in aligning their policies, strategies and management frameworks with them.[38]

At the global regulatory level, discussions are under way as to whether financial capital is an appropriate measure to mitigate cyber risk.[39] For example, in the scenario of an institution affected by a ransomware attack that encrypts the entirety of its critical systems,

---

34 According to AON's 4th annual study on cyber security and cyber risk management in Spain 2023 (only available in Spanish), between 2017 and 2020 the number of cyber insurance claims in Spain quadrupled.

35 See the FSB report *Effective Practices for Cyber Incident Response and Recovery* of October 2020.

36 See the FSB report *Format for Incident Reporting Exchange (FIRE)* of April 2023.

37 See *Principles for Operational Resilience,* March 2021.

38 See the *BCBS Supervisory newsletter on the adoption of POR and PSMOR* of November 2023.

39 L. F. Signorini. (2021). "Implementing Basel III in the EU: remaining challenges and timing". *Eurofi Magazine.*

the institution's survival would depend on whether or not it has technical measures in place that can allow it to recover. Financial capital would not be the main determinant of resilience in this case, although it could affect the ability to finance the roll-out of these technical measures. In less extreme events, with partial loss of systems, greater solvency may be of greater relative benefit, as institutions would have more options to take actions requiring funding. In any case, it is necessary to assess whether the additional resilience to cyber risk provided by a certain amount of financial capital can be more efficiently achieved by accumulating more technological resources. Moreover, many experts disagree on whether or not technology-related risks should be a sub-category of operational risk, given their cross-cutting nature, which has become more pronounced as the digital transformation has progressed.

Regulation and supervision act as catalysts for financial institutions to properly manage cyber risk. Many jurisdictions such as the EU, the United Kingdom,[40] the United States[41] and Australia[42] have consequently developed regulatory and supervisory frameworks and tools in this area.

The EU has been host to intense regulatory activity to address cyber risk. The 2016 Network and Information Security Directive (NISD), on measures for a high common level of security of network and information systems, was a clear commitment by the EU to improve cyber security in all national critical sectors, including credit institutions and market infrastructures. The Directive has been overhauled and replaced by the NIS 2 Directive, which expands its scope and must be transposed into the national legislation of Member States by October 2024. Other recent regulations could also be mentioned here, such as the Directive on the resilience of critical entities,[43] the cyber security Regulation,[44] and the draft cyber resilience Regulation.[45]

The EU's financial system has more regulations on cyber risk than any other. Other sectoral rules include the EBA's 2017 Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process[46] (SREP) and its Guidelines on ICT and security risk management,[47] which have served as benchmarks ever since they were released. Relationships with third parties have also been in the EBA's spotlight, evidenced by the publication of its

40 *Operational resilience of the financial sector,* Bank of England.

41 See the Federal Reserve's annual *Cybersecurity and Financial System Resilience Report,* the Cybersecurity and Infrastructure Security Agency's *Cyber Resilience Review* and the National Institute of Standards and Technology's *Cybersecurity Framework 2.0* report.

42 See Cyber Security, Council of Financial Regulators.

43 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

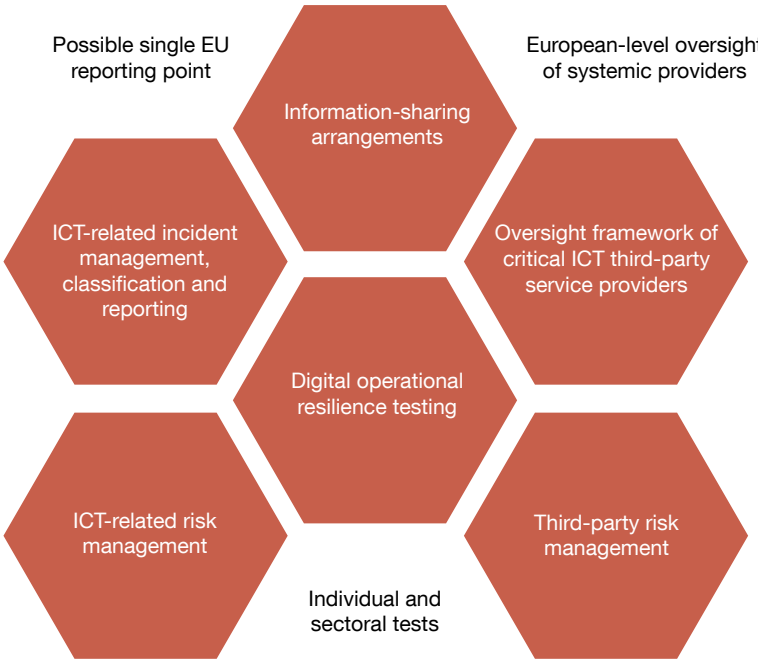
44 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the EU Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

45 Draft Cyber Resilience Act.

46 EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (EBA/GL/2017/05).

47 EBA Guidelines on ICT and security risk management (EBA/GL/2019/04).

Figure SF.1
Main parts of DORA



SOURCE: Banco de España

Guidelines on outsourcing arrangements in 2019.[48] In the area of market infrastructures, the European Central Bank (ECB) published its expectations for cyber resilience in 2018,[49] based on the guidelines published in 2016 by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions.

DORA will be a turning point for the cyber resilience of the EU's financial system from its application in January 2025. This Regulation is part of the European Commission's digital finance strategy and its aim is to mitigate the risks associated with digitalisation and strengthen the resilience of the European financial system. It includes requirements for financial institutions on managing technology-related risks, managing technological incidents and notifying supervisors, testing of systems' resilience and managing relations with third parties (see Figure SF.1).

In addition to its microprudential scope, DORA also addresses certain aspects of the systemic dimension of cyber risk. To do so, it promotes information sharing between institutions and establishes mechanisms for cooperation between authorities within and beyond the financial system (both supervisory authorities and non-financial sector ones, such

48 EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

49 See the ECB report Cyber resilience oversight expectations for financial market infrastructures of 2018.

as security agencies); orders a feasibility study of a single incident reporting point for all European financial institutions; and establishes an oversight framework for those technology providers that are critical for the European financial system.

In the area of microprudential supervision, financial authorities in the European banking sector have incorporated cyber risk into both ongoing monitoring and on-site inspections of institutions and horizontal activities. To this end, these authorities have been equipped with specialised resources and have laid down methodologies and working procedures adapted to the specific features of this risk. In addition, most of them have established reporting requirements for major cyber incidents so that potential adverse events that may require some form of intervention by the authorities can be detected as early as possible.

Beyond the strictly supervisory approach, many authorities have established cyber resilience testing frameworks based on threat intelligence. These tests seek to simulate a sophisticated and as-realistic-as-possible cyber attack on an institution's operational systems, drawing on intelligence on the most likely attackers and their techniques and procedures. The aim is to assess the institutions' technical, human and organisational capabilities to detect and react to the attack without the defence being forewarned of any such test. The authority monitors all stages of the test to check that the requirements of the framework are met. In the case of the EU, 16 jurisdictions, including Spain, have already adopted the ECB's TIBER-EU testing framework.[50]

SF.3.2 Managing cyber risk at financial institutions

In response to the increasing volume and sophistication of cyber threats, as well as regulatory and supervisory requirements, financial institutions are pushing to improve their cyber risk management. Many of them rely on market standards and best practices, and sometimes specialist consultancy firms, to improve their technical measures and cyber resilience. This involves working on prevention aspects and detection capabilities as well as on the procedures and solutions needed to respond to a cyber incident and, if necessary, recover from its impact. Given the complexity of institutions' systems and the rapid pace of technological developments, sustaining this effort over time poses a challenge for many of them, leading to varying levels of cyber resilience.

Financial institutions have shifted towards a more holistic approach, focusing not only on technology but also on the human factor and organisational aspects. Thus, in addition to the constant updating and improvement of technical measures, significant efforts have been made to train employees and raise their cyber security awareness in order to prevent their exploitation as an attack vector. Similarly, awareness and understanding of cyber risk among institutions' senior management has grown in recent years, and the second and third

50 See the information on the ECB website on the TIBER-EU framework.

lines of defence (i.e. the risk management and compliance functions and the audit function, respectively) have been strengthened in this area.

In the same vein, financial institutions have worked to raise awareness among their customers of the importance of cyber security. The digitalisation of financial services has led to a shift of traditional fraud towards digital channels, using social engineering techniques to mislead customers. Institutions carry out frequent training and awareness-raising campaigns to help customers detect and prevent such attacks, as well as to safeguard and protect their credentials and devices, but these are not enough. Cooperation with other actors, such as telecommunications providers, is also required, e.g. to prevent attacks based on fraudulent duplication of SIM cards or phishing campaigns.

Cyber resilience is based on the assumption that cyber incidents will occur and that they can lead to disruptions to critical services, from which it will be necessary to recover. This is why institutions establish and test their business continuity plans, envisaging an array of adverse scenarios, including cyber attacks. Moreover, they conduct crisis management simulations to check that the procedures in place are adequate throughout the entire incident simulated. Some of these exercises take into account the concentration in the technology provider sectors, in particular cloud services, and the resulting difficulty in substituting services in the event of an incident.

SF.3.3 Assessment and management of systemic risk linked to cyber risk

From individual to systemic

In recent years financial authorities have also started to focus on the systemic implications of cyber risk. While the regulatory and supervisory spotlight was initially aimed at managing and assessing cyber risk at the individual level, the increase in the sector's technological dependence, as well as the number and impact of cyber incidents, have made it necessary to address cyber risk from a systemic perspective. Although the earliest publications on the systemic aspect of cyber risk predate 2020,[51] there is a significant increase in studies from that year onwards.

In 2017 the ESRB set up a dedicated task force to study cyber risk's potential impact on financial stability: the European Systemic Cyber Group. As a result of this group's work, the ESRB published a number of reports analysing the impact propagation model for cyber incidents that could jeopardise financial stability[52] and proposing tools for the assessment and mitigation of systemic cyber risk.[53, 54]

---

51 For example, *Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system* (2017), *Cyber Risk, Market Failures, and Financial Stability* (2017), *The Future of Financial Stability and Cyber Risk* (2018), *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment* (2019).

52 See the ESRB report *Systemic cyber risk* of 19 February 2020.

53 See the ESRB report *Mitigating systemic cyber risk* of 27 January 2022.

54 See the ESRB report *Advancing macroprudential tools for cyber resilience* of 14 February 2023.

The various studies and analyses carried out on the systemic aspect of cyber risk share a number of important conclusions. First, assessing cyber risk and its impact at a systemic level is complex. Quantifying impacts is difficult even at the level of an individual institution, but attempting to do so at a systemic level is far more complex. Another important aspect is the need for authorities to have systemic cyber incident response plans and regularly review and test them. Finally, ensuring close coordination between authorities is seen as a crucial element for managing systemic cyber incidents.

Latest initiatives

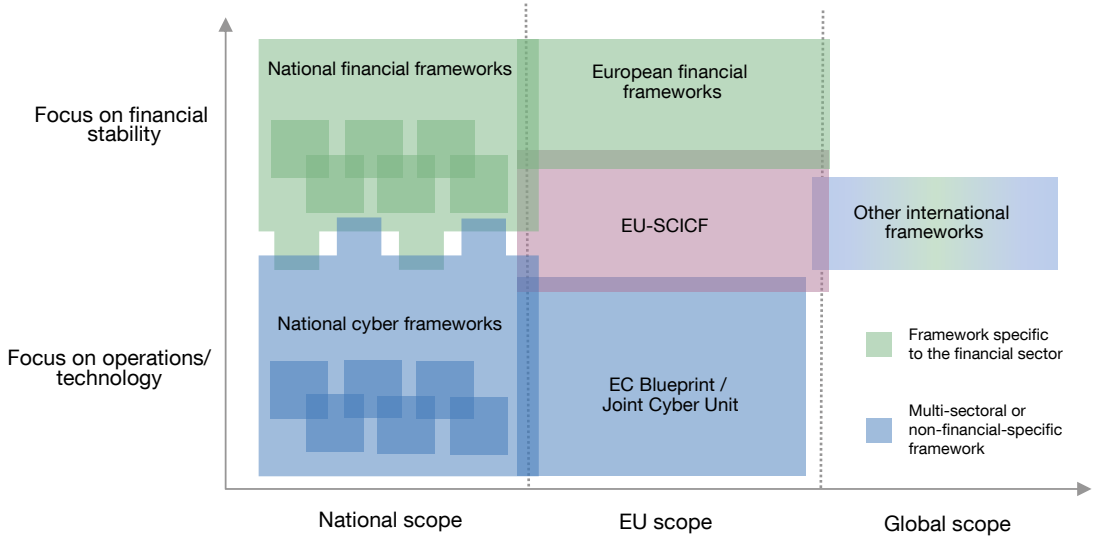
In the EU, a significant portion of the most recent initiatives relating to the systemic component of cyber risk focus on measuring its impact. The ESRB has done some notable work in this area, such as developing the Systemic Impact Tolerance Objective (SITO).[55] Estimating and analysing the SITOs for different economic functions can help in the complex task of assessing cyber risk at the systemic level. Owing to their application at the macroprudential level, SITOs differ from previous approaches to resilience and technological risk, such as the Recovery Time Objective (a measure of the time during which an individual organisation can tolerate systems not operating and the associated drop in service levels without compromising business continuity).

SITOs define the point after which the financial system as a whole is unable to absorb the impact of a systemic cyber incident. Establishing these measures will help authorities understand the conditions under which a crisis may be triggered during an ongoing systemic cyber incident They also aid in setting thresholds below such points and conditions, which are related to a certain amount of deterioration, so that institutions can react and try to mitigate impacts before they trigger a broader crisis. A SITO could be defined for a specific economic function based on the number of affected transactions, their value in euro, the duration of the cyber incident and the number of affected institutions and jurisdictions. Thus, insofar as a cyber incident could spread to different institutions and jurisdictions (if, for example, they all used the same application that has been compromised by cyber criminals), it could last longer, affect more transactions and, consequently, have a costlier impact. This would increase the overall impact of the cyber incident, potentially reaching a point where financial stability would be compromised. The high degree of concentration among technology providers, which limits alternative choices in the event of failure, may, under certain circumstances, increase the probability of SITO thresholds being exceeded, as well as the speed at which that could happen, and thus the supervisory focus on them.

Operationalising SITOs poses some conceptual challenges. The ESRB has provided some principles to direct these efforts. In particular, SITOs should reflect impacts on all economic functions that may be affected by cyber risk and account for the interconnections

55 See the ESRB report *Advancing macroprudential tools for cyber resilience* of 14 February 2023.

Figure SF.2
Frameworks for coordination between authorities dealing with cyber risk



SOURCE: ESRB. (2022). *Mitigating systemic cyber risk.*

between these functions and across jurisdictions and sectors of economic activity. These metrics should capture the varying severity and duration of the events and should also be easy to communicate and reviewed on a regular basis.

Also noteworthy is the ESRB recommendation to establish a pan-European systemic cyber incident coordination framework. The aim is to fill the gap between cyber incident management frameworks at European level that focus on financial stability and those specifically focused on the technical and operational response (see Figure SF.2). The potential scale and contagion speed of systemic cyber incidents required a framework that would enable financial authorities to react swiftly and flexibly at European level, something that does not seem feasible with what is currently in place.

The ESRB also studied cyber resilience test scenarios[56] at a systemic level. The ESRB proposes this type of test in its report as a new tool to, among other things, enable an assessment of the financial system's ability to absorb shocks from systemic cyber incidents that could potentially affect financial stability. The cyber risk scenarios for these tests are focused on operational issues, in contrast to the macro-financial scenarios used in traditional stress tests, and can provide a framework for combining different tools and capabilities to manage cyber risk.

Furthermore, DORA encourages authorities to organise crisis and contingency management exercises that include cyber attack scenarios. The aim is to gradually enable

56 Cyber Resilience Scenario Testing (CyRST).

an effective coordinated response at EU level. The ECB is conducting a cyber resilience stress test[57] on all its supervised institutions in 2024. The importance of these tests is also illustrated by the implementation of sector-specific exercises by the authorities[58] and industry.[59]

Macroprudential tools and other systemic actions taken by financial authorities to address cyber risk

The macroprudential tools included in current banking sector regulations were not specifically designed to address external non-financial threats, such as cyber risk. However, the potential disruptive consequences[60] of a cyber incident for the financial system as a whole may warrant the release of previously accumulated macroprudential capital buffers so that banks can continue supplying credit to the economy. Thus, the macroprudential toolkit could be adapted to deal with cyber risk. For example, the systemic risk buffer could be applied differently to banks based on their level of technological systemicity. This could help limit the occurrence of systemic events and subsequent contagion events. This is, however, an issue which is at a very preliminary stage and still requires significant research before more detailed policy recommendations can be adopted in the future.

The materialisation of cyber incidents with a significant financial impact may require financial instruments to be used for crisis management. A financial crisis, regardless of its origin, can be managed using existing instruments, including deposit insurance, moratoria or special liquidity injections, as long as their conditions of use are tailored to the technological and risk context. A cyber incident could cause a bank to limit operations, 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 risk that the incident may pose to financial stability and allowing them to continue providing services to the economy.

Similarly, bank resolution frameworks can also be useful in these scenarios. Resolution and recovery plans, while not specifically designed for such situations, may be modified to ensure the continuity of the critical functions of banks potentially affected by the incident.

It should be noted that the conditions of application of financial instruments must be modified in light of the technological context of the risks.[61] Simultaneous disruptions in operational and financial areas warrant combined approaches to action. The availability of

---

57 See the ECB press release *ECB to stress test banks' ability to recover from cyberattack*.

58 For example, the Bank of England's exercises with industry partners (SIMEX), *SIMEX 22 – A two-day market wide simulation exercise exercise to test the UK financial sector's resilience to a major operational disruption*.

59 The exercises organised in Spain by the Centro de Cooperación Interbancaria, for example, or the ISMS Forum, The ISMS Forum puts the cyber resilience capabilities of 35 Spanish firms to the test at the Cross-sector Cyber Exercises (only available in Spanish).

60 Beyond the initial operational difficulties they may cause, cyber incidents also undermine the profitability of financial institutions and, potentially, their liquidity and solvency. As a result, credit supply could be impaired in the wake of a cyber incident.

61 José Ramón Martínez Resano. (2022). *Digital Resilience And Financial Stability. The Quest For Policy Tools In The Financial Sector.*

adequate technological resources may be a necessary condition for applying the traditional financial resources (e.g. emergency liquidity and the aforementioned resolution framework) to address these cyber incidents. These technological resources comprise the software, hardware, know-how and specialised staff that enable institutions to effectively and efficiently manage their ICT systems and, in particular, guarantee their security and cyber-resilience. Increasing technological resources may be the most efficient way to limit systemic cyber risk by significantly reducing the financial impact of cyber incidents.[62] Investing in the modernisation and replacement of legacy ICT systems is acutely important here.

Two possible examples that need to be explored are the introduction of circuit breakers and the use of cross-institution collective support mechanisms that allow the system as a whole to share technological resources. The first measure involves suspending processes in the event of simultaneous technological and financial crises. This freeze allows more data on the nature of the crisis to be gathered so that the financial and operational response can be better targeted. The second would make it possible to implement redundancy and security in the system, thus enabling cross-bank collaborative restructuring of processes should one fail or, similarly, providing data access (via a data vault) if one bank's data are compromised in an isolated cyber attack.

SF.4 Conclusions and outlook

The digitalisation of society, the economy and the financial system will proceed apace, forcing all actors in the financial system, including supervisory and regulatory authorities, to step up their work on cyber risk. This adaptation will require the necessary technical roles to be recruited and incorporated into organisations in sufficient numbers, meaning that attracting and retaining talent will remain a challenge for the sector, especially for smaller institutions.

The potential of artificial intelligence will equip both cyber attackers and defence teams with new tools. Content generation capacities, whether text, voice or image-based, will facilitate identity theft and make social engineering attacks much more credible. Artificial intelligence can also help to create malware and optimise attacks. At the same time, it allows defence teams to identify cyber threats at an early stage by recognising patterns from the analysis of large volumes of near-real-time information. It is also possible to partially automate responses, thus complementing the work of analysts and substantially shortening reaction times.

The possibilities offered by quantum computing[63] mean that many current encryption methods will be breached in the medium term. This affects the confidentiality of encrypted

62 For example, a cyber incident that completely paralyses the financial system has a high economic cost per unit of time. Investing in technological resources that reduce the likelihood of such an occurrence may be more efficient and feasible than accumulating capital equivalent to the losses in these types of incidents.

63 Quantum computing uses quantum mechanics laws to solve complex problems that cannot be solved by classical systems.

information, including backups, as current thefts of encrypted data could provide the attacker with decrypted information in the future. It also affects most authentication mechanisms and, therefore, data integrity, as false credentials could be created and authentic private keys fraudulently obtained. This could lead to the alteration of legal history via tampering with signed documents or the creation of validly signed falsified documents. Work is already under way[64] to create cryptographic algorithms resilient to quantum computing and to plan the migration of hardware, software and services using potentially vulnerable cryptography to such hardened algorithms.

From the perspective of the financial system's cyber resilience, initiatives are under way to ensure that critical data can be recovered in the event of a major incident. Data vaulting strategies include offline and offsite storage of the information that an institution needs to operate its critical services. The most advanced example is Sheltered Harbor,[65] which involves and is supported by the main US banking associations. Participating institutions send their encrypted data in an agreed format to shared data vaulting facilities so that their data can be recovered and processed on a recovery platform, should the need arise. Potential micro- and macroprudential data vaulting requirements could be a useful element of cyber risk regulation and supervision, but the issue is still at an early stage.

Sharing data on cyber threats and incidents is key to improving collective defence capabilities. Technical details of a cyber attack that has had an impact on one institution can help others protect themselves against a similar attack. There are already numerous forums in the financial system allowing data sharing, both industry-specific[66] and involving authorities.[67] The central role of authorities, which under DORA will receive reports of cyber incidents from the institutions under their remit, will allow them to feed back useful information to the industry.

Similarly, sectoral cyber resilience tests and crisis management exercises and even getting other sectors involved will be key in the coming years. It will be necessary to guarantee not only the response and recovery capacity of each financial institution, but that of the system as a whole. Doing so will involve carrying out sector-specific tests that include the participation of the appropriate providers. Ideally, where operational inter-dependencies exist with other sectors, they will need to be integrated into such tests in the future. This inclusion would be done gradually, as these sectors reach the proper level of maturity. The authorities will have to play a fundamental coordinating role in the event of a crisis. It is therefore essential that they encourage and are involved in the conduct of such exercises.

Further progress is needed on the quantification and understanding of cyber risk for financial stability and the potential role of macroprudential policies in mitigating them.

64 See the competition organised by the US National Institute of Standards and Technology for post-quantum cryptography standards.

65 See the Sheltered Harbor website.

66 The FS-ISAC, for example.

67 The Cyber Information and Intelligence Sharing Initiative, for example.

Financial interconnections are a complex subject of analysis and the digitalisation process has expanded these networks with new agents, such as technology providers. This transformation requires assessing the potential role in cyber risk mitigation of traditional macroprudential measures (e.g. capital buffers) and also the extent to which requirements for technological resources (e.g. data vaulting, operational resilience tests) may substitute them more effectively and efficiently.