Cyber risk as a threat to financial stability

Francisco José Herrera Luque

BANCO DE ESPAÑA

José Munera López

BANCO DE ESPAÑA

Paul Williams

PRUDENTIAL REGULATION AUTHORITY (UK)

Francisco José Herrera Luque belongs to the Cybersecurity Unit of the Directorate General Services of Banco de España, francisco(dot)herrera(at)bde(dot)es; José Munera López belongs to the IT Risk Division of the Directorate General Banking Supervision of Banco de España, jose(dot)munera(at)bde(dot)es; and Paul Williams is Head of the Operational Risk and Resilience, Supervisory Risk Specialists Division of the Prudential Regulation Authority (UK), paul(dot)williams(at)bankofengland(dot)co(dot)uk.

Resumen

Los sistemas de información desempeñan un papel esencial en el funcionamiento de las entidades financieras. Si bien estos sistemas sustentan los servicios de las entidades y facilitan sus estrategias, sus vulnerabilidades subyacentes podrían constituir una importante fuente de riesgo, el ciberriesgo. Este tipo de riesgo puede afectar a las capacidades de las entidades financieras e incluso poner en peligro su viabilidad. Además, como consecuencia del elevado grado de interconexión e interdependencia entre los elementos del sistema financiero, el ciberriesgo podría contagiarse entre entidades. Por consiguiente, la materialización del ciberriesgo en su forma más extrema podría suponer una amenaza para la estabilidad del sistema financiero.

Para abordar esta cuestión, en este artículo se presentan, en primer lugar, los ciberincidentes y sus costes estimados, centrando la atención en el sistema financiero. A continuación, se caracteriza el ciberriesgo, así como las principales vulnerabilidades y amenazas para la ciberseguridad que afectan a las entidades financieras. Este análisis va seguido de una explicación del posible impacto sistémico del ciberriesgo sobre el sistema financiero, basada en el uso de modelos teóricos. También se presentan aspectos destacados del marco regulatorio actual en materia de ciberriesgo de aplicación a las entidades financieras que operan en España y, por último, se examinan las líneas de trabajo futuras recomendadas para mejorar la gestión del ciberriesgo en el sistema financiero.

Abstract

Information systems play a critical role in the functioning of financial institutions. While supporting their services and enabling their strategies, underlying vulnerabilities could pose an important source of risk: cyber risk. This may impair financial institutions' operational capabilities and even threaten their viability. Furthermore, the high level of interconnection and interdependence between the elements of the financial system allows for the contagion of cyber risk among them. Consequently, the materialization of cyber risk in its most extreme form could threaten the stability of the financial system.

To address this topic, the article first introduces cyber incidents and their estimated costs, focusing on the financial system. Cyber risk is then considered, together with the main vulnerabilities and threats to cyber security affecting financial institutions. This is followed by a justification of the potential systemic effect of cyber risk on the financial system, supported by the use of theoretical models. Moreover, highlights of the current regulatory framework on cyber risk for financial institutions operating in Spain are also presented. Finally, recommended future lines of work for the improvement of the management of cyber risk in the financial system are discussed.

1 Introduction

Perhaps the most notorious cyber incidents to date are the WannaCry and NotPetya *ransomware*[1] cyber-attacks. The WannaCry attack in May 2017 affected computer systems in more than 150 countries,[2] while the NotPetya attack in June 2017 is possibly the most destructive cyber-attack ever seen, with an estimated cost of US$10bn according to a US White House assessment.[3] Although not aimed at the financial sector, these attacks affected banks, ATM networks and card payment systems.

Indeed, multiple organizations of different sizes across different sectors have recently been targeted by ransomware attacks. Notably, in the last half of 2020, two of the most relevant Spanish insurers.[4,5] The attack suffered by one of them impacted

1 A cyber-attack designed to block access to an information system and/or the information it stores until a sum of money is paid.

2 Reuters: Cyber-attack hits 200,000 in at least 150 countries: Europol - See news article.

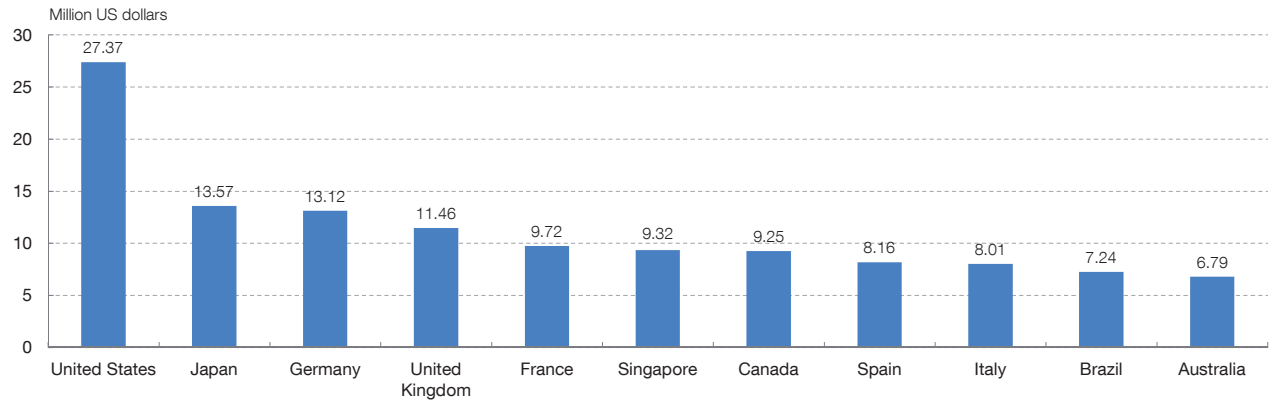
3 Wired: The Untold Story of NotPetya, the Most Devastating Cyberattack in History - See news article.

4 Spanish National Cybersecurity Institute (INCIBE): Mapfre suffers from ransomware cyberattack - See highlight.

5 *El País:* How a ransomware attack impacted one of the biggest Spanish insurers - See news article in Spanish.

Chart 1

ESTIMATED AVERAGE ANNUAL COST OF CYBER-ATTACKS IN LARGE ORGANIZATIONS (a) PER COUNTRY



SOURCE: *Ninth Annual Cost of Cybercrime Study,* conducted by Accenture and Ponemon Institute (2019).

a In the context of the study, large organizations are those with a number of employees greater than 5,000.

90% of its information systems while for the other, it took more than six weeks to recover the functionality of its systems.

The financial sector has long been a key target for cyber criminals looking for financial gain (and not only). For many years, the majority of financial institutions has traditionally been targeted through *phishing*[6] and banking *malware*[7] – in addition to other cyber threats[8] –, and still are.

Despite the fact that **the total cost of cyber incidents is notoriously hard to establish,** it seems clear that their impact on organizations, industries and the society as a whole is substantial. Chart 1 illustrates the estimated average annual cost of cyber-attacks for large organizations according to a study[9] conducted in 355 companies across eleven countries. In the case of Spain, it reaches the value of $8.16M.

Chart 2 illustrates that the financial sector suffers the highest average costs of cyber-attacks compared to other sectors.

According to the same study, large organizations belonging to the financial services industry have to afford the highest costs of cyber-attacks per organization, with an estimation of $18,37 M, while the banking industry follows closely, with $17,84 M.

6 Any fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising as a trustworthy entity in an electronic communication.

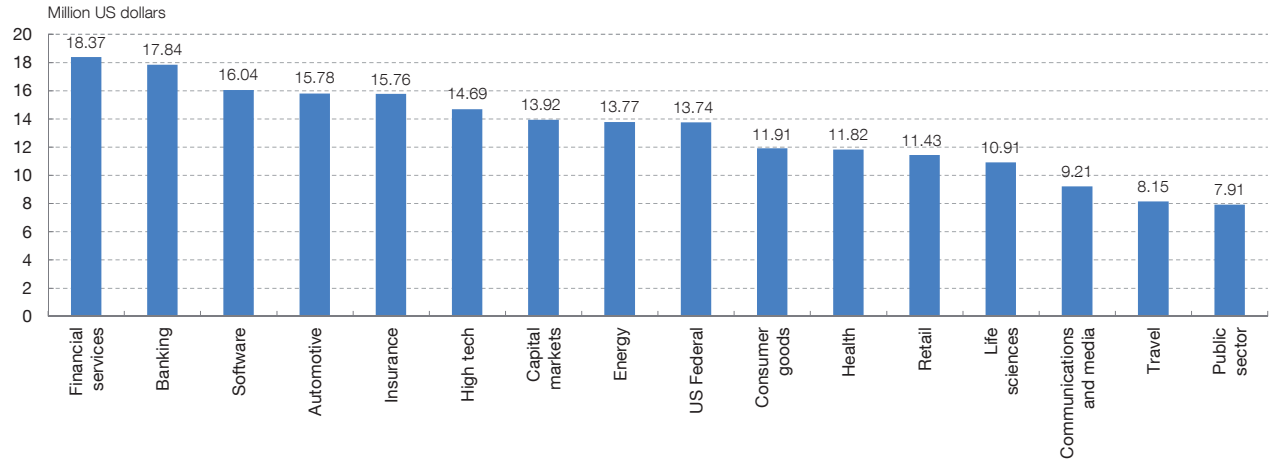
7 Any software intentionally designed to cause damage to information systems.

8 Additional examples of cyber incidents affecting financial institutions can be found at the compilation performed by the Carnegie Mellon Cyber Policy Initiative, available here.

9 See Accenture and Ponemon Institute (2019).

Chart 2

ESTIMATED AVERAGE ANNUAL COST OF CYBER-ATTACKS IN LARGE ORGANIZATIONS PER INDUSTRY



SOURCE: *Ninth Annual Cost of Cybercrime Study,* conducted by Accenture and Ponemon Institute (2019).

Insurance industry organizations are in the fifth position, with an estimation of $15,76 M, while those belonging to capital markets category have to face $13,92 M costs on average per year.

The volume, severity and sophistication of cyber-attacks on institutions are on the rise. During 2019, 67% of financial institutions experienced an increase in the number of cyber-attacks; 26% of the attacks had the aim of being purely destructive, which represented a 160% increase compared to the previous year.[10] Furthermore, 79% of cybersecurity directors of the world's leading financial institutions claim that cyber criminals have become more sophisticated.

But **cyber incidents can also happen without the intervention of malicious threat actors.** A notable example of this occurred in April 2018 at a Spanish owned British bank, after the migration of its IT platform.[11] After three years of planning and testing, the bank migrated its data and operations to a single new IT platform. Despite the successful migration of customer and financial data, infrastructure and software issues led to significant levels of instability in the new platform. These issues ultimately led to disruption in the bank's online and mobile banking services as well as its call centres and branches.

Banco de España is Spain's national authority responsible for prudential supervision of credit institutions, within the framework of the Single Supervisory Mechanism,

10 See VMware (2019).

11 The report of an independent review by Slaughter and May, commissioned by the bank, can be found here.

and other supervisory tasks and, as a central bank, seeks to promote the proper functioning and stability of the Spanish financial system and of the national payment systems, without prejudice to the functions of the ECB. In this context, **cyber risk is an emerging area of interest for** the fulfilment of its mandate. In addition, the recent transposition into the Spanish legal framework of the Directive (UE) 2016/1148 on network and information systems security (known as NIS Directive) appoints **Banco de España** as a national competent authority for credit institutions.[12]

There is an increasing interest in understanding the potential impact of cyber risk on financial stability and improving the resilience of the financial system in the event of a systemic cyber event. This article introduces the problem of cyber risk from the perspective of the financial sector at both the individual institutions and system-wide level. In the absence of previous events, the potential effect of cyber risk on financial stability is justified supported by the use of models. An analysis of the characteristics of the regulatory framework for the cyber risk affecting the financial sector in Spain is made in order to address the missing elements required to safeguard financial stability against this type of risk.

2 Cyber risk and financial institutions

Data is paramount for financial institutions to provide their services. Financial institutions'[13] data rely on the proper and reliable functioning of information systems. These systems form the backbone of almost all their processes and distribution channels as well as supporting the automated controls environment that assure information integrity. They also bring new opportunities to improve traditional businesses and generate new ones.

Information systems represent material proportions of institutions' costs, investments and intangible assets.[14] Their importance to financial institutions' operations means they also become sources of fragility should these systems fail or the data become unreliable. They are therefore, attractive targets for malicious actors and pose additional risks to the institutions.

As illustrated in previous examples, **cyber incidents are events that compromise the security of information systems and the information they hold,** regardless of

12 According to the Royal Decree 43/2021, published on the 26th of January 2021, which develops the Spanish legislation transposing Directive (UE) 2016/1148 on network and information systems security (known as NIS Directive). Available here.

13 In the context of this article the concept of financial institution covers, among others, financial intermediaries, markets and market infrastructures.

14 By June 2020, the European Parliament voted to allow banks to include the value of their software systems in the calculation of their reserves – something worth tens of billions of euros for the sector – as part of the adjustments in response to the COVID-19 pandemic. The European Banking Authority has been charged with finding a common method of valuation. Available here.

Table 1

SECURITY PROPERTIES GIVING RISE TO CYBER RISK AS DEFINED IN THE CYBER LEXICON DEVELOPED BY THE FINANCIAL STABILITY BOARD (FSB) (a) AND EXAMPLES OF CYBER INCIDENTS RELATED TO THEIR COMPROMISE

Definition of the security properties giving rise to cyber risk	Examples of cyber incidents related to their compromise
Confidentiality: information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems	Financial institution's clients accessing the financial positions of other clients
Integrity: accuracy and completeness	Data stored and processed by information systems are incomplete, inaccurate or inconsistent across different systems
Availability: being accessible and usable on demand by an authorized entity	Disruption of online banking services as a consequence of a information system failure
Authenticity: an entity is what it claims to be	Illegitimate replication of online banking services for the performing of phishing campaigns
Accountability: ensures that the actions of an entity may be traced uniquely to that entity	Inability to identify the originator of a transaction
Non-repudiation: ability to prove the occurrence of a claimed event or action and its originating entities	A customer of a financial institution orders a transaction that is not carried out. The customer cannot prove that his order was received by the institution
Reliability: consistent intended behavior and results	Information system instability as a consequence of a technological platform migration

SOURCE: Authors' elaboration.

a See Financial Stability Board (2018).

whether they originate from intentional attacks – cyber-attacks – or not. **Cyber risk can be defined as the combination of the probability of cyber incidents occurring and their impact.** A definition of the security properties giving rise to cyber risk is provided in Table 1, being confidentiality, integrity and availability the primary ones.

Technology is obviously crucial when it comes to cyber risk; however, this risk is not only about information systems, **but also processes and people.** It is not possible to deploy and rely on technology and maintain a reasonably guarded security posture without competent people and suitable support processes, encompassing management systems, best practices and governance frameworks, including IT audit.

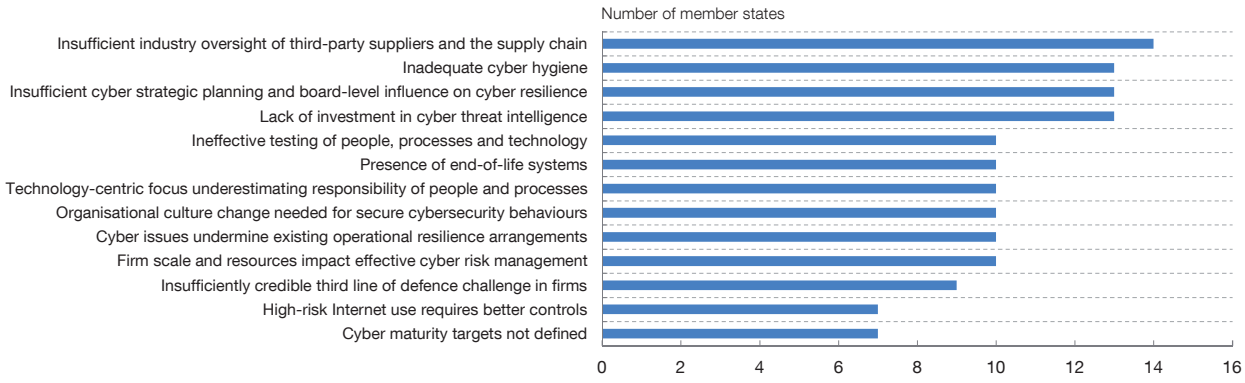
Although cyber risk can be viewed as a subset of operational risk,[15] it differs in material ways from more traditional sources of operational risk.

Cyber risk related assets – namely people, processes and technology – can present (and they inevitably do) weaknesses, susceptibilities or flaws, which are known as vulnerabilities. **Cyber risk materialises in cyber incidents through the exploitation of these vulnerabilities.**

15 Operational risk encompasses the risk of financial losses stemming from inadequate or failed internal processes, people and systems or from external events.

Chart 3

PREVALENCE OF COMMON CYBER VULNERABILITIES IN 14 EU MEMBER STATES FINANCIAL INSTITUTIONS



SOURCE: European Systemic Cyber Group, *Report on the systemic characteristics of cyber risk.*

Chart 3 shows a set of thirteen common cyber security vulnerabilities in European financial institutions belonging to 14[16] EU member states ranked according to their frequency of occurrence[17] across them. The information was gathered as part of the European Systemic Cyber Group's work (ESCG).[18]

Of particular concern is that **human actors with malicious intent can cause cyber risk materialize.** These actors are typically grouped into (i) hostile nation-states – whose capabilities are increasingly sophisticated when compared to other actors –, (ii) terrorist groups moving into the cyber arena, (iii) cybercrime organizations – generally interested in making profit through cyber-attacks –, (iv) hacktivists – motivated by political demands –, (v) disgruntled employees that exploit their privileged access to organization's IT resources, and (vi) individual malicious intruders, known as hackers.

Threats to cyber security have a fast paced evolving nature. No wonder, then, a plethora of public and private organizations issue cyber threats assessment reports to track their evolution relatively frequently.[19] According to these reports, the financial sector is usually among the most exposed to these threats. Notably,

16 Belgium, Germany, Hungary, Ireland, Italy, Lithuania, Malta, The Netherlands, Poland, Romania, Slovenia, Spain, Sweden and the United Kingdom (at the time member state of the EU).

17 This, however, does not imply the severity of the vulnerabilities or mean that a particular vulnerability has materialised in the jurisdiction concerned, only that it has been noted to exist.

18 The European Systemic Cyber Group (ESCG) is an experts group established by the European Systemic Risk Board (ESRB) in 2017 to investigate systemic cyber risk and examine whether and how a cyber-incident could cause a systemic crisis. Since 2020 the ESCG is arranged as a joint ESRB-Bank of England working group.

19 A reference for the reader could be those issued by ENISA, the European Union Agency for Cybersecurity, available here, and by the CCN-CERT, one of the Spanish national governmental agencies on cybersecurity, available here.

financial institutions fall under the interest of different kinds of malicious threat actors that have been identified to date and **threats to the cyber security of financial institutions have a specific profile**.[20]

Financial institutions have **complex and interdependent supply chains** that offer a broad, target-rich attack surface that adversaries can undermine. Despite the fact that attackers have been conducting supply chain attacks for years, in December 2020 an unprecedented sophisticated global scale cyber-attack[21] leveraging SolarWinds Orion IT software was unveiled.[22]

Credentials and identity theft compromise and abuse have traditionally been cornerstones for targeted attacks and fraud. As a consequence of the COVID-19 pandemic, financial institutions have been forced to rapidly adjust their operations to enable massive and swift telework deployment. From the point of view of technology, this has implied an expansion of the attack surface, potentially increasing vulnerabilities further.

Data theft is also among the traditional threats to the financial institutions. Recently, threat actors are often going beyond theft to include data destruction and disruption. A new wave of cyber-attacks sees data no longer simply being copied, but also destroyed — or changed — breeding distrust.[23]

As technology advances, both cyber-defenders and adversaries are exploring means of using new tools. An example, on the threat actor side is the use of *deepfake*[24] technologies to increase the effectiveness of their campaigns. **Disinformation and misinformation campaigns** are of particular concern in this regard. Notably, multiple United States entities, including the NASDAQ, Securities Exchange Commission and FINRA have warned of spikes in market manipulation in the wake of the COVID-19 pandemic. Often, market manipulation involves elements of disinformation or misinformation directed at influencing unsuspected investors to aid criminal actors' objectives. Malicious actors can take advantage of high market volatility which could further undermine market confidence.

It is important to note that **not every cyber incident is the result of an intentional attack,** such as those originating from natural disasters disrupting IT infrastructure or accidental actions of authorized IT systems users. In fact, some of the biggest data breaches have been caused by poor IT systems configuration.

---

20 According to the SecurityHQ white paper "Financial Sector Threat Landscape 2020". Available here.

21 Reuters: SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president news article.

22 The first statement made about its detection is available here.

23 Indeed, destructive and disruptive malware attacks are on the rise and cross-sector targeting and threat groups leveraging ransomware are targeting multiple related parties at once globally.

24 An artificial intelligence technique that allows to edit fake videos of people who are apparently real, using unsupervised learning algorithms and existing videos or images.

The high level of interconnectedness of information systems enables cyber incidents to be more widespread in their impact than many other shocks. Additionally, the high level of automation of information systems enables cyber incidents to spread rapidly, making human intervention difficult. Thus cyber risk has the potential to materialize and propagate at a significantly quicker pace than other types of risk.

Regardless of whether they originate from intentional attacks or not, **cyber incidents typically result in business disruption, information loss, equipment damage or even in revenue loss.** Given the dependence of financial institutions on information technology, the performance of economic functions[25] by financial institutions could be affected by cyber incidents.

Finally, **the scale and complexity of organizations' IT infrastructure makes impossible their absolute protection and elimination of cyber risk.** Consequently, cyber incidents may have a high degree of inevitability. In fact, cyber incidents have the potential to impair the operational capabilities of financial institutions to a point that compromises their viability.

3 Cyber risk can threaten financial stability

Initially, it may seem that cyber risk is only a threat to the soundness of financial institutions individually. On the contrary, **the interdependence of the information systems supporting the financial system further enables cyber incidents to spread to organizations not initially affected.** In the worst cases, an incident can spread widely across sectors and even beyond geographical borders.

Assessing the potential impact of cyber risk on financial stability[26] is a complex task since there are no historical examples from which to draw lessons or conclusions. However, the lack of examples cannot be considered proof that cyber risk cannot impact financial stability.

In its 2017 report: *Cybersecurity and Financial Stability: Risks and Resilience,* the U.S. Office of Financial Research (OFR) identifies **three potential ways in which cyber incidents can threaten financial stability: lack of substitutability, loss of confidence and loss of data integrity.** Lack of substitutability can be seen from a financial system perspective (e.g. a clearing house) or from a technological perspective (e.g. a main cloud service provider).[27]

25 See Financial Stability Board (2013).

26 For the purpose of this article the definition for financial stability used is the one published by the ECB here: "Financial stability can be defined as a condition in which the financial system – which comprises financial intermediaries, markets and market infrastructures – is capable of withstanding shocks and the unravelling of financial imbalances. This mitigates the prospect of disruptions in the financial intermediation process that are severe enough to adversely impact real economic activity."

27 See Healey et. al (2018a).

In its 2020 report, the ESCG built upon those potential ways a cyber incident could threaten financial stability and defined a set of **characteristics**[28] **that make the financial system vulnerable to cyber risk:** a high degree of interdependence, the absence of a clear view of those dependencies, a high level of reliance on data and the relevance of confidence.

The **high degree of interdependence** can come in the form of dependencies between different components of the system (e.g. between financial institutions or between them and market infrastructures) but also between components of the system and those from outside the system (e.g. software or communication services providers). A cyber incident in a particular component could spread to others that depend on it regardless of whether they are part of the financial system or not.

There is a **lack of understanding around the concentration and dependency of relationships between components** of the financial system, and also those components from outside the system. This hinders the ability to fully understand how, for example, an impact on a certain service provider can spread within the financial system.

High reliance on data makes any impact on the confidentiality, integrity or availability of data (the three main information security focus points) susceptible to wide-spread consequences in the system; for instance, unavailability or tampering of trading prices can stop a market from operating.

Confidence is key in the financial system and can become crucial in a financial crisis, as we have seen in the past; it takes time to build it but can be destroyed in minutes. Cyber incidents and the uncertainty that may come with them can quickly erode confidence and have a widespread impact on the system. For example, a cyber incident that corrupts account balance data of a bank, even for a short period of time, will have a sizeable impact on the confidence in the institution.

In order **to assess the potential impact a single component might have on the whole system** the FSB has established three criteria[29] that can be applied both in the financial and technological domains: size, substitutability and interconnectedness.

Size is an intuitive criterion: a cyber-incident in a component of the system that represents a significant percentage of it can affect the whole system.

The **lack of substitutability** of certain core components of the financial system, like critical financial market infrastructures (e.g. clearing and payment systems), generate

28 See European Systemic Cyber Group (2020).

29 See International Monetary Fund/Bank for International Settlements/Financial Stability Board (2009).

single points of failure. It is more likely that a cyber-incident affecting one of such components can lead to a system-wide impact.

Interconnectedness between components of the financial system is a key criterion when assessing the potential propagation a cyber-incident might have through the system. Notably, information technology has substantially increased the level of interconnectedness between components of the financial system (and of them with external elements), both technically and financially.

Taking into account the characteristics of cyber risk, previously discussed in this article, and the aforementioned characteristics of the financial system, it is possible to begin understanding how the **crystallisation of cyber risk can have a considerable impact at a system-wide level.** However, this doesn't imply that a cyber-incident, even if it has a sizeable impact and a system-wide reach, has the potential to compromise financial stability.

In order to make this link, and in the absence of previous financial stability crises originated by cyber incidents, a deeper analysis of how these characteristics interact is needed. Both qualitative and quantitative approaches are useful tools to have a better understanding of the potential impact of cyber risk on financial stability.

Quantitative models can provide numerical estimations of cyber risk impacts but they require sufficient data from previous events in order to be accurate. The Federal Reserve Bank of New York (FRBNY) published a report featuring a quantitative approach to the impact of a cyber-incident.[30] The report adds a valuable approach to existing literature by providing a detailed description of the economic impact a cyber-attack can have in the U.S. wholesale payments network.

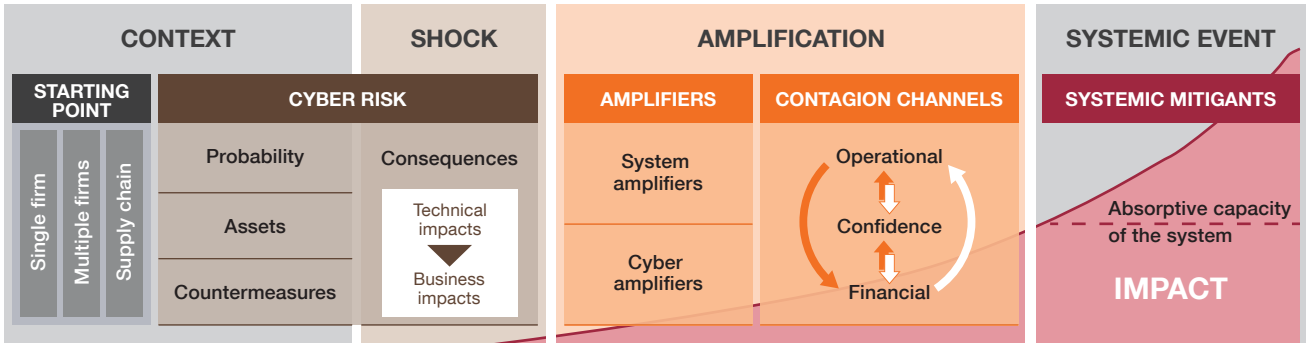
Using real wholesale payments data from 2018, the report estimates that a cyber-attack impacting any of the five most active US banks could lead to the impairment,[31] on average, of 38% of the payment network. The forgone payment activity could be up to 2.7 times the daily United States GDP; and up to a 30% higher if the cyber incident occurs on certain dates with higher payment volumes.

This model provides actual cost estimations of the impact that a cyber-incident with system-wide effects can have, demonstrating their potential negative effects to financial stability. However, it does not focus on the mechanisms that allow a cyber-incident to become amplified to the point in which it begins having a significant impact.

30 See Eisenbach et al. (2020).

31 Impairment of an institution is defined in Eisenbach et al. (2020) as the point at which "the counterfactual end-of-day reserve balance is more than two standard deviations below its average, over a 30 day window."

Figure 1
A MODEL FOR THE PROPAGATION OF CYBER INCIDENT EFFECTS IN THE FINANCIAL SYSTEM



SOURCE: Authors' elaboration. Adapted from the model presented in Ross (2020).

Qualitative approaches on the other hand give us a better understanding of the factors and mechanisms that come into play when cyber risk crystallises and how these mechanisms and factors can amplify its effects to the point in which it may threaten financial stability. Analysing each step of this process and how different elements come into play during the amplification of a cyber-incident, helps us identifying system vulnerabilities relevant to cyber security (in contrast with those at a single institution level) as well as potential mitigants that could help prevent financial stability issues arising from a cyber-incident.

A conceptual model is a more appropriate tool to explore how cyber risk and the financial system can interact in such a way that financial stability is affected. Following a similar approach as previous works,[32] the ESCG developed a conceptual model[33] **to analyse the evolution of cyber incident effects from its inception, considering three contagion channels that spread its effects: operational, confidence and financial.**

The model, based on the FSB's approach to macro-financial implications of operational and cyber risk, **divides the analysis of the evolution of a cyber-incident to its final outcome in four phases: context, shock, amplification and systemic event,** as shown in Figure 1.

The **context phase** analyses the risks that can crystallise and lead to a cyber-incident and provides the complete context under which a cyber-incident arises. This analysis includes not only the threat classification of the crystallised risks (localisation, motivation and agent) but also the assets affected (financial and non-financial), the capacity of the organisation to mitigate cyber risk as well as the starting

32 See Kaffenberger and Kopp (2019), and Healey et al. (2018b).
33 See Ross (2020).

point, i.e. single institution hit by an incident, multiple financial institutions hit simultaneously or via the supply chain.

In the **shock phase** the immediate impacts of the cyber incident are assessed. This phase does not take into account the likelihood of the shock and focuses instead on the technological and business impacts generated by the loss of one or more of the cyber security properties mentioned before (confidentiality, integrity and availability being the primary ones) as a result of the cyber incident.

The **amplification phase** makes use of two concepts: **amplifiers** that can increase the impact or likelihood of the shock (distinguishing between system amplifiers and cyber specific amplifiers), and **contagion channels** through which the shock can be transmitted (confidence, financial and operational). These two concepts are brought together to explore how the affected financial institutions interact with their systems and how the initial shock propagates.

The last phase of the model, **systemic event phase,** evaluates the point at which a cyber-incident becomes systemic; that is the point at which the system is no longer able to absorb the shock. To identify this point, an upper impact tolerance threshold for the financial system has to be defined (i.e. the point at which the aggregate impact becomes too great for the system to bear). The model also introduces a lower impact threshold, below which individual institutions, the services they provide, and the economic functions they support, should operate within. The gap between both represents the absorptive capacity of the system, the coping capacity within the system to absorb shocks.

In order to better illustrate how a cyber-incident can impact the financial system, the abovementioned model can be applied against a hypothetical scenario developed by the ESCG.[34] The scenario is based on the destruction or alteration of value-related data (e.g. account balances) as a result of a cyber-attack to the account data and payment software of a large bank. Figure 2 details the development of the incident through the phases of the model.

The application of ESCG's conceptual model to this scenario suggests **there are potential mitigants that could help reduce the impact of the incident.** The main contagion channels in this scenario are financial and confidence. Public concern about their savings can easily extend to customers of all banks, while uncertainty about the problem and its solution erodes confidence not only within the public, but also within other market participants and authorities. At the same time, the financial impact spreads from the bank to its counterparties, causing liquidity problems.

34 See European Systemic Cyber Group (2020).

Figure 2

APPLICATION OF ESCG'S CONCEPTUAL MODEL TO A HYPOTHETICAL SCENARIO

Propagation of the effects of the destruction or alteration of value-related data (e.g. account balances) as a result of a cyber attack to the account data and payment software of a large bank			
Context phase	Using malicious software and infiltrating the IT systems management supply chain, threat actors gain access to certain IT systems of a bank. For several months, undetected, they have performed reconnaissance tasks while gaining access to critical systems as well as to backup and restoration processes. The attackers then initiate the execution of a massive set of fraudulent payments, covering their tracks by deleting the account balance data of a large number of accounts as well as payment-related processes and software		
Shock phase	Unsure of what the problem is, the bank suspends its payment operations. Short-term solutions (e.g. manual workarounds) are deployed, but their viability depends on how long they will have to be used. Concerns are raised about the reliability of the live data as it becomes clear that the incident affects the bank's subsidiaries in other countries via their shared IT systems. The incident is communicated to the National Competent Authority of the countries impacted		
Amplification phase	Unaware of the full extent of the attack, of the possible impacts in the backup and restoration procedures and of the time that will be required to resume services, the bank initially assumes that activity could be resumed before manual workarounds become unviable. As time goes by, critical activities exceed their maximum tolerable downtime thresholds and the bank begins to set up alternative platforms to operate. Contagion between the following different channels begins:		
Operational to operational contagion	Operational to financial contagion	Operational to confidence contagion	Confidence to confidence contagion
Appears when it becomes evident that restoration will not be possible as the attackers were able to alter backup and recovery procedures. The interdependencies between account balances, payment systems and treasury procedures impacts treasury services, and by the end of the first day the bank's receipts and payments are pending	Follows when institutional customers of the bank do not receive expected payments. Customers are also unable to use funds from their deposits. The bank's management starts considering the possibility that data will not be recovered in a short period of time or even that the data may have been permanently lost The bank's financial position starts to deteriorate as it cannot perform payment, clearing or settlement services A more severe scenario could have been created if the attackers had hindered the capacity of the bank to receive emergency liquidity from the central bank by incapacitating its collateral framework, thus triggering default management procedures or even the intervention of resolution authorities	Arises as customer are increasingly unable to withdraw funds (both at ATMs and branches). Customers seek to understand the impact of the problem and how long it will last, as they try to ascertain whether their money is safe	Could occur in a more severe scenario if the attackers claim responsibility for the incident and threaten to repeat it in other banks. This claim, added to the existing concern, could have a larger impact if the use of social media to spread rumours amplifies the erosion of confidence in the financial system
Systemic event phase	Although some data could be recovered in the short term, it becomes apparent that full data recovery will require a semi-manual process, which will take a considerable amount of time. As a result of this, the bank notifies authorities, markets and its customers of the situation. While the bank and its counterparties begin to report liquidity problems, disruptions begin in the payment, clearing and settlement systems of the country. While financial institutions request help from authorities, loss of confidence spirals as customers try to move their funds out of the bank, but the unreliable balances make it almost impossible. Fear that this event has impacted other banks spreads, increasing concerns across the financial sector. The authorities consider different actions like establishing a communication strategy to offer reassurance to the public. The lack of previous experience dealing with similar crisis adds to the uncertainty experienced by authorities, market participants and customers		

SOURCE: Authors' elaboration. Adapted from European Systemic Cyber Group (2020).

As the scenario progresses, a better understanding of its impact and spread develops. It is therefore possible to reflect on how some of the events could have been prevented or mitigated. Would a critical data backup provided by the authorities have allowed the bank to restore data and resume operations faster? How could the impact on liquidity have been mitigated? What would have been the impact of a social media campaign spreading false rumours? How could financial institutions

and authorities increase or keep market and public confidence during the incident? Raising these kind of questions and seeking answers to them can be helpful in shaping effective policies to mitigate the impact of cyber risk.

The conclusion drawn by the ESCG from the application of the conceptual model to different scenarios[35] (both real and hypothetical) is that **in order to have a significant impact on financial stability, a cyber-incident must:**

- Be of **intentional nature,** a cyber-attack, with a clear intention to cause damage.
- Be **carried out by actors with sophisticated capabilities.**
- Have a **specific alignment of amplifiers and lack of effective mitigants.**
- Create actual or anticipated **losses** that **cannot be absorbed, which erode trust** in and within the financial system.

ESCG's conclusions add on to a growing consensus considering that cyber risk has the potential to have a significant impact on financial stability. However, how to predict and measure the impact are still subject of analysis. Whether agreeing with the same specific factors defined by the ESCG or defining new ones, it becomes evident that, **given a set of specific concurrent factors, cyber risk can threaten financial stability.**

This convergence of factors should not be considered proof of the low probability of this kind of cyber incident happening. Unintentional cyber incidents have the potential to impair an institution. If combined with an impact in the confidence channel due to, for example, a malicious social media campaign, there remains the possibility of a financial stability impact. Furthermore, an increase in the capabilities of threat actors, due to black-market propagation of sophisticated tools, combined with increasingly complex IT systems, creates a rapidly evolving technological risk landscape where the probability of high-impact events increases.

4 Cyber risk regulatory framework for Spanish financial institutions

Regulators have been working for years on implementing strategies to address cyber risk. In the past decade, supervisory best practices and tools have been established **focused on single institutions soundness.** Regulatory frameworks have been developed to identify, evaluate and mitigate cyber risks for financial institutions, but also to help them prepare to respond to cyber incidents.

35 See European Systemic Cyber Group (2020).

Traditionally, European regulators have addressed cyber risk with a fragmented approach, including dispositions on Information Technology as part of different sectorial regulations (e.g. the Payment Services Directive, PSD2,[36] which has dispositions on cyber risk but only covers payment service providers).

The following is a brief outline of three of the most important European regulations for the financial system defining obligations in order to enhance cyber security: the directive on the security of network and information systems (NIS Directive), the General Data Protection Regulation (GDPR) and the revised Payment Services Directive (PSD2).

The NIS Directive[37] (NISD) is the first piece of EU-wide legislation purely focused on cyber security. It pursues the objective of improving the security of networks and information systems underlying either digital services providers or essential services operators, which includes the most relevant institutions of the financial sector. It aims to improve cyber security capabilities at national level, and to enhance cooperation in order to facilitate and improve cyber incident response activities. To do so, it mandates the development of a National Cyber Security Strategy[38] and the designation of a Single Point of Contact, National Competent Authorities and Computer Security Incident Response Teams (CSIRTs).

The **General Data Protection Regulation**[39] (GDPR) entered into effect in May 2018, **setting new and unprecedented data privacy and security standards.** Financial institutions are affected by this regulation so long as they target or collect data related to people in the European Union or offer services to them. Among other provisions, GDPR requires the handling of personal data securely, by implementing "appropriate technical and organizational measures" and envisages fines that can be up to four percent of the offending organization's global profits.

The revised Payment Services Directive (PSD2), transposed to the Spanish regulatory framework in November 2018, updates the previous payment services directive. The main goals pursued with this update are **fostering innovation and competition in the European payments market while improving the security of transactions and data.** This regulation poses new challenges for institutions regarding cyber risk given that, while including several cyber security technical requirement (e.g. strong costumer authentication[40] or transaction and device

36 See *Payment services (PSD2) - Directive (EU) 2015/2366.*

37 See Directive on security of network and information systems (NISD) - Directive (EU) 2016/1148.

38 The last version of the Spanish National Cybersecurity Strategy is available here (only in Spanish).

39 See *General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679.*

40 "An authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data", PSD2, Article 4(30).

monitoring), it also increases their attack surface by requiring them to develop an external access interface to payment accounts for third parties.

Looking at the regulation issued by the three European Supervisory Authorities (ESAs) fragmentation is also present. The banking sector, as spearhead of technology adoption in the financial system, has a more developed and extensive regulatory framework on cyber risk. Examples of this are several guidelines and regulatory technical standards issued by the European Banking Authority (EBA) in the last years[41] (e.g. the EBA Guidelines on ICT and security risk management). Also ESMA and EIOPA[42] have recently published guidelines dealing with aspects of cyber risk (e.g. EIOPA Guidelines on information and communication technology security and governance[43] or ESMA Guidelines on outsourcing to cloud service providers[44]).

In Spain, banks are subject to a wide range of national and European Union regulations. When it comes to cyber risk, banks have requirements coming from: (i) different regulations for specific activities (e.g. PSD2 for the payment services they provide); (ii) regulation with a wider scope for the banking sector (e.g. the EBA Guidelines on ICT and security risk management); or (iii) more general regulation that covers different sectors (e.g. the General Data Protection Regulation, GDPR, and its local adoption[45] in relation to personal data or the Network Information Security Directive and it local transposition[46]).

Regulatory fragmentation poses several problems, both for authorities and financial institutions. For authorities, for example, fragmentation makes it difficult to have a clear overview of the whole financial sector regulatory framework, what regulations are in place and affect different financial institutions, etc. This also may hinder authorities' coordination capabilities when responding to a cyber-incident since it will be difficult for them to know other authorities that should be involved, their responsibilities, points of contact, requirements for financial institutions, etc.

Fragmentation can become a problem for those financial institutions who are subject to different regulations. For example, a bank that is victim of a cyber-attack affecting personal information of its payment services clients will have to report the event to different authorities, both national and European (including data protection agencies, law enforcement, local Computer Emergency Response Teams – CERT –, local supervisors and the ECB) to comply with its obligations under different regulations (e.g. PSD2 for the payment service perspective or GDPR from the personal data

41 See *EBA Guidelines on ICT and security risk management* (EBA/GL/2019/04).

42 The European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

43 See *EIOPA Guidelines on information and communication technology security and governance.*

44 See *ESMA Guidelines on outsourcing to cloud service providers.*

45 See Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales.

46 See Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

perspective). That reporting will also have to be done taking into account different requirements (i.e. thresholds, formats, timeframes) making compliance even more burdensome in a moment where efforts should be focused on managing the incident.

Being aware of this and of other burdens that regulatory fragmentation may pose to both authorities and financial institutions, **regulators are in the process of increasing the level of harmonization in cyber risk regulation.** Initiatives like the Digital Operational Resilience Act[47] (DORA) or the Revised Directive on Security of Network and Information Systems[48] (NIS2) are clear examples of how regulators are trying to address the issue.

In addition, authorities are sponsoring initiatives to better understand cyber vulnerabilities in the financial sector and interdependencies between financial institutions. They are also paying attention to contagion risk, trying to understand how impacts derived from a cyber-incident could spread among multiple institutions, affecting financial stability.

5 Reducing the impact of cyber risk on financial stability

Cyber risk requires a concurrent approach from both micro- and macro-prudential angles. The risk arising from the aggregate impact of cyber risk at individual institutions makes **microprudential policies an essential tool in reducing the potential threat to financial stability.** Cyber risk is not a novelty in microprudential regulation and there are already policies that deal with this risk from different angles.

By contrast, **macroprudential policies,** which are typically aimed at mitigating and preventing cyclical or structural systemic risks to financial stability, **have not focused on cyber risk to date.** This can be partially explained by the fact that cyber risk has only been seen as a type of operational risk and has therefore been managed from a microprudential perspective. Another reason could be that no actual cyber incident has had a profound system-wide impact on financial stability yet.

Existing macroprudential tools may not prove effective for dealing with issues derived from a cyber-incident as macroprudential policies are basically conceived to be deployed in a preventive manner. For example, capital buffers or liquidity tools may not be the right levers in preventing a systemic event if a G-SIB loses its account balance data due to a cyber-incident. Similarly, such tools may prove to be ineffective if a critical financial market infrastructure suffers a cyber-incident that forces it to cease operations for a prolonged period.

47 See legislative proposal for an EU regulatory framework on digital operational resilience for the financial sector – Digital Operational Resilience Act (DORA).

48 See proposal for directive on measures for high common level of cybersecurity across the Union - Network and Information Systems (NIS 2 Directive).

Cyber risk can also crystallise at a speed and scale that might render existing instruments unsuitable for competent authorities. The uncertainty of the origin, intent and impact of a cyber-incident can make authorities' reactions insufficient and inadequate when dealing with system-wide confidence.

In order to lessen the potential impact of cyber risk on financial stability and improve the financial system resilience, authorities will have to act. We believe that **legislative improvements should be introduced, both at micro- and macro-prudential levels,** to:

— Improve coordination between authorities during cyber incidents.

— Gain a better understanding of cyber risk's potential impact on financial stability.

— Enhance preparation and foster information sharing both at institutions and authorities level.

— Reduce the aggregated impact of cyber risk at individual level.

— Increase regulatory harmonization.

Improving coordination between authorities is key when dealing with the impact of a risk that has such a rapid crystallisation ability and diverse manifestation like cyber risk.[49] To achieve this, a common coordination framework will be required. At the base of this framework should lie a common lexicon and taxonomy with agreed threshold and classification criteria.

While the lexicon will ensure that information is interpreted adequately by all authorities, the taxonomy will allow incidents to be classified homogeneously across all jurisdictions, reducing potential discrepancies. Among other key elements of a coordination framework we could mention common information sharing formats, secure communication channels or well identified points of contact for all involved authorities.

The complexity of the financial system requires a deeper level of understanding in order to build on the work done in creating and analysing different cyber risk scenarios.[50] To better understand cyber risk's potential impact on financial stability we must first have a clear view on the financial sector's interdependencies,[51] both at technical and operational level.

49 See Oliver Wyman and Depository Trust and Clearing Corporation (2018).

50 See Boer and Vázquez (2017), and Kaffenberger and Kopp (2019).

51 See Ross (2020).

Creating a sectorial map of these interdependencies is a complex task that authorities may want to approach on a bottom-up basis, beginning with simpler maps at national level that are then aggregated and analysed at European level. This approach would allow national authorities to have a clear view on their jurisdictions dependencies, while at the same time European authorities would achieve an overarching view.

Improved quantitative and qualitative models would be another paramount tool to improve our understanding of cyber risk's potential impact and how interdependencies, amplifiers and mitigants interact in a cyber-incident.[52]

Authorities not only have to develop adequate instruments to deal with a cyber-incident (e.g. common coordination framework, common taxonomy and lexicon, interdependencies maps or predefined actions plans for certain scenarios); they also have to be sure that they can use them efficiently and build up their capabilities and those of the financial institutions.

Preparation of the financial sector can be driven by authorities by establishing periodical cyber exercises in local jurisdictions and at cross-national level. Although there are crisis exercises performed in the financial sector, they still are a fragmented effort since they usually have a limited scope (e.g. Financial Market Infrastructures, single jurisdictions, individual financial institutions or not considering certain aspects of a cyber-crisis). Also, there is not a comparable level of maturity among jurisdictions. Periodical cross-national cyber exercises may encourage countries to conduct regular exercises within their jurisdiction.

Information sharing, as a cornerstone of coordination, is crucial to enable a collective system-wide response to cyber risk.[53] Authorities and regulations are increasingly focused on information sharing,[54] alongside other organisational initiatives that focus on information sharing like the Financial Services Information Sharing and Analysis Center (FS-ISAC[55]) or the UK's Cross Market Operational Resilience Group.

Trust is a key element when it comes to information sharing. Financial institutions may not be inclined to share confidential details about cyber incidents with its competitors or supervisors. To foster information sharing between financial institutions and authorities, obstacles to it (e.g. limitations imposed by regulations or national security agencies, lack of trust between parties or confidentiality and liability concerns) must be overcome.

---

52 See Ross (2020), Kaffenberger and Kopp (2019), and Healey et al. (2018b).

53 See Oliver Wyman and Depository Trust and Clearing Corporation (2018).

54 See World Bank (2020), and Basel Committee on Banking Supervision (2018).

55 See FS-ISAC web page.

Authorities should help build a trust network that fosters information sharing across the financial sector. To do so, it is our opinion that encouraging voluntary sharing is the best option, whether it is between financial institutions, between authorities or between financial institutions and authorities. All parties should agree a common set of rules and formats to share information and an open dialogue must be established to discuss what barriers are identified and how they can be overcome (e.g. changes in legislation, setting up secure information sharing mechanisms or creating public-private collaboration forums).

As mentioned earlier in this article, there are already **microprudential policies** that deal with cyber risk, and their **evolution is crucial** to better reflect expectations from regulators and guidance from international bodies[56] and to adapt to new technologies and circumstances.[57]

The first three regulatory principles presented in Kashyap and Wetherilt (2019) show how microprudential policies can be a catalyst for improving individual institutions' risk management: (i) insist that firms operate with the presumption that a successful high-impact attack is inevitable; (ii) insist that firms plan for prolonged and system-wide disruption, with particular attention to resourcing for response and recovery; and (iii) aim for a two-way dialogue between firms and supervisors as part of a wider collaborative approach to recovery objectives.

All these lines of action must follow an overarching principle of **regulatory harmonization.** Regulatory fragmentation will not only hinder the aforementioned improvements suggested, it has a clear negative impact on coordinating, gaining a clear overview of the financial system, sharing information or understanding the aggregated impact of individual risks. It is paramount that further legislative improvements are aligned, with recent efforts to enhance regulatory harmonization like the European Commission initiatives DORA and NIS2. This means focusing on regulatory initiatives with a wider scope rather than on specific aspects or activities of the financial sector.

6 Conclusions

Information systems are a key resource for developing and supporting **financial services** as well as enabling financial institutions' strategies. This important role along with some features of the financial system (i.e. interdependencies and the difficulty in achieving a clear view on them, reliance on data and on confidence) make cyber risk a potential threat to financial stability.

56 See G7 (2016), and Crisanto and Prenio (2017).

57 See Kopp et al. (2017).

The financial sector is a traditional victim of cyber-attacks. Studies show that the average annual cost related to these malicious cyber incidents is particularly high in this sector. A closer look onto malicious cyber incidents reveals new attacks discovered every month, with an increasing severity and sophistication.

Cyber risk is different to other forms of operational risk. While directly linked with technology, persons and processes play also a vital role in it and they all present the vulnerabilities that give rise to cyber risk. These vulnerabilities are exploited by cyber threats, sometimes specifically tailored for the financial sector, including, among others, data thefts, identity thefts, supply chain attacks and data encryption. Even if a cyber-incident at individual institutions does not pose a risk to the whole system, it can impair the institution's capabilities and even compromise their viability.

The financial sector is highly reliant on data and confidence; it also features a high degree of interdependence between its components and there is no clear view on those dependencies. These intrinsic characteristics make **the financial sector particularly vulnerable to cyber risk and confers this risk the potential to impact financial stability.** In order to assess the potential impact of cyber risk, quantitative and qualitative models are being developed, each with different advantages and disadvantages.

One of these models is the conceptual model developed by the ESCG, based on the FSB's approach to macro-financial implications of operational and cyber risk. The model can be applied to real and hypothetical scenarios to understand how a cyber-incident can spread and evolve to become a systemic event and which mitigants could help reduce its impact. The ESCG concluded from the application of the model that in order to threaten financial stability, a cyber-incident would require a specific convergence of factors.

Both microprudential and macroprudential policies are paramount to reduce the potential impact of cyber risk on financial stability. While cyber risk has been under the microprudential policies' focus for some time, this has not been the case for macroprudential policies, which remain to be further developed in several areas. One possible explanation could be the lack of actual cases of a cyber-incident impacting financial stability since the introduction of macroprudential tools in financial regulation. In addition, the characteristics of cyber risk may render existing macroprudential tools ineffective when applied to issues stemming from cyber-incidents.

Cyber risk is becoming an increasingly important area of attention for authorities with capacity to issue regulation for the financial sector[58] **or**

58 Financial institutions may also be affected by cyber security regulations issued by non-financial authorities at both national and supra-national levels.

influence in it. The effort carried out ranges from high level principles issued by fora like the G7[59] or the Basel Committee on Banking Supervision (BCBS),[60] European initiatives like Digital Operational Resilience Act[61] (DORA) and the Revised Directive on Security of Network and Information Systems[62] (NIS2) to more detailed guidelines like those issued by the European Banking Authority (EBA). Even though the current regulatory framework for cyber risk still lacks a harmonized approach, through initiatives like DORA or NIS2, authorities aim to reduce the regulatory fragmentation affecting cyber risk.

Given the intrinsic characteristics of the financial sector and cyber risk as well the current status of regulation and policies, we are of the opinion that **additional efforts should be made to lessen the impact of cyber incidents on financial stability.** Despite authorities increasing attention on cyber risk, we think that there is still room for legislative improvements in order to:

- Enhance coordination between authorities during cyber incidents.
- Gain a better understanding of cyber risk's potential impact on financial stability.
- Enhance preparation and foster information sharing both at institutions' and authorities' level.
- Reduce the aggregated impact of cyber risk at individual level.
- Increase regulatory harmonization.

59 See G7 (2016) and G7 (2018).

60 See Basel Committee on Banking Supervision (2018).

61 See legislative proposal for an EU regulatory framework on digital operational resilience for the financial sector – Digital Operational Resilience Act (DORA).

62 See proposal for directive on measures for high common level of cybersecurity across the Union - Network and Information Systems (NIS 2 Directive).

REFERENCES

Accenture and Ponemon Institute (2019). *Ninth Annual Cost of Cybercrime Study.*

Basel Committee on Banking Supervision (2018). *Cyber-resilience: Range of practices,* Bank for International Settlements.

Boer, M., and J. Vázquez (2017). *Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system,* Institute of International Finance, Washington, DC.

Crisanto, J., and J. Prenio (2017). «Regulatory approaches to enhance banks' cyber-security frameworks», *FSI Insights on policy implementation,* No. 2, Financial Stability Institute, Bank for International Settlements.

Eisenbach, T. M., A. Kovner, and M. J. Lee (2020). *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis,* Federal Reserve Bank of New York Staff Reports, Report No. 909.

European Central Bank (2016). *Stocktake of IT risk supervision practices*.

European Systemic Cyber Group (2020). *Systemic cyber risk,* European Systemic Risk Board.

Financial Stability Board (2013). *Guidance on Identification of Critical Functions and Critical Shared Services.*

Financial Stability Board (2018). *Cyber Lexicon*.

G7 (2016). *Fundamental Elements of Cybersecurity for the Financial Sector,* G7 Cyber Expert Group.

G7 (2018). *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector,* G7 Finance Ministers and Central Bank Governors.

Goh, J., H. Kang, Z. X. Koh, J. W. Lim, C. W. Ng, G. Sher and C. Yao (2020). *Cyber Risk Surveillance: A Case Study of Singapore,* Working Paper No. 20/28, International Monetary Fund.

Healey, J., P. Mosser, K. Rosen and A. Tache (2018a). *The Future of Financial Stability and Cyber Risk,* Cybersecurity project at Brookings, the Brookings Institution, Washington, DC.

Healey, J., P. Mosser, K. Rosen and A. Wortman (2018b). *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.

International Monetary Fund/Bank for International Settlements/Financial Stability Board (2009). *Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments: Initial Considerations,* Report to the G-20 Finance Ministers and Central Bank Governors.

Kaffenberger, L., and E. Kopp (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., and A. Wetherilt (2019). «Some Principles for Regulating Cyber Risk», *AEA Papers and Proceedings,* 109, pp. 482-487, American Economic Association.

Kopp, E., L. Kaffenberger and C. Wilson (2017). *Cyber Risk, Market Failures, and Financial Stability,* Working Paper No. 17/185, International Monetary Fund.

Office of Financial Research (2017). *Cybersecurity and Financial Stability: Risks and Resilience,* Viewpoint February.

Oliver Wyman and Depository Trust and Clearing Corporation (2018). *Large-scale cyber-attacks on the financial system. A case for better coordinated response and recovery strategies,* white paper.

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.

VMware (2019). *2020 Cybersecurity Outlook Report,* March, VMware Carbon Black Threat Analysis Unit.

World Bank (2020). *Financial Sector's Cybersecurity: A Regulatory Digest,* July, Financial Sector Advisory Center, World Bank Group.