Strengthening the cyber resilience of the financial sector. Developments and trends

Silvia Senabre, Iván Soto and José Munera

BANCO DE ESPAÑA

The authors belong to the Directorate General Banking Supervision of the Banco de España, and are grateful for the comments received from an anonymous referee. Email for comments: silvia(dot)senabre(at)bde(dot)es.

Abstract

The debate about the cyber resilience of the financial sector has become more important in recent years. In this article the authors endeavour to clarify the meaning of this concept and why it has become a topic of growing concern for financial institutions and authorities. They analyse how cyber resilience in the financial sector has evolved in recent years, its current situation and the trends observed. Lastly, they define the way in which the different actors involved work towards enhancing it. In particular, they describe the various regulatory and supervisory actions conducted by the sectoral authorities in this field.

Keywords: resilience, operational resilience, cyber resilience, cyber security, cyber incident.

1 Introduction

In recent years references to resilience have become a common topic in all kinds of publications, speeches[1] and debates, both for the authorities and for the private sector, a trend which has been exacerbated by the COVID-19 pandemic. But what does resilience mean?

The term "resilience" comes from the field of psychology and, although there is no single definition, it is usually understood as the ability to adapt to adverse situations. Different terms have derived from this general concept for their use in other fields. One of the most common, particularly relevant from the perspective adopted in this article, is "operational resilience", which the Basel Committee on Banking Supervision (BCBS) defined in its Principles for Operational Resilience[2] 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 sector.

In an increasingly digitalised world where information and communication technologies (ICT) play a key role in financial operations, the fact that cyber resilience has emerged as a specific case of operational resilience comes as no surprise. This article shall use as a reference the Cyber Lexicon of the Financial Stability Board (FSB),[3] which defines cyber resilience as the ability of an organisation to continue to

1 See Hernández de Cos (2019).
2 See BCBS (2021a).
3 See FSB (2018).

carry out 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. This definition encompasses both the cyber security component, which is more preventive, and the business continuity component, which focuses on response and recovery when incidents occur.

The definition of cyber incident in the FSB's Cyber Lexicon refers to events resulting from both non-malicious and malicious activity (caused by cyber attacks). In the latter case, which includes events such as natural disasters, human errors or accidental system failures, they may also affect the ability of institutions and the sector to continue operating normally. Accordingly, resilience to these cyber incidents is equally important. However, the article will analyse intentional incidents in greater depth, given their higher potential impact.

The financial sector is a very complex ecosystem, with numerous participants (including market infrastructures, financial institutions and providers) which are closely interconnected and interdependent, and which have different levels of maturity in terms of cyber resilience.

Some of the financial sector's intrinsic characteristics not only generate a high level of exposure for individual institutions to cyber incidents, but may also help extend or amplify their impact to an extent that could jeopardise financial stability.[4] These characteristics include its strong dependence on technology, its appeal to attackers with different motivations, the high degree of interconnectedness among its members and its high sensitivity to participants' loss of confidence.[5]

For this reason, improving the financial sector's cyber resilience is key for preserving financial stability. This article describes some of the main initiatives that have been or are being carried out by both the private sector and the authorities to help fulfil this objective, with a special focus on those directly affecting the Spanish financial sector.

2 Background

2.1 Digitalisation and exposure to cyber risk

Historically, the financial sector has been very proactive in the use of information technologies to set in place new business models and optimise internal processes. This digital transformation process has accelerated extraordinarily in recent years, becoming essential for the survival of institutions, for various reasons.

4 See Herrera, Munera and Williams (2021).

5 See ESRB (2020).

First, changes in the expectations of customers, who value the availability of flexible services that are tailored to their needs and are immediately accessible anywhere and on any device. This has been reinforced by the emergence of new competitors for traditional institutions, such as BigTech[6] and FinTech[7] firms, which provide customers with highly attractive solutions and are quick to develop new offers.

In addition, the low interest rate economic environment has led institutions to adapt their business models, launching new products and services in their search for alternative sources of income and improving the efficiency of their internal processes to cut costs. All this while harnessing the rapid developments in technology, which have made it possible to multiply systems' capacities while reducing prices.

As a result, the financial sector is highly digitalised, to the point that institutions are completely dependent on their technology, not only as a facilitating instrument for the business, but as a differential and competitive factor. Evidently, the high level of digitalisation increases the risk of cyber incidents (both those caused by system failures and malicious incidents or cyber attacks). Other factors contributing to this increasing risk include the complexity of most financial institutions' technological environment. Thus, legacy applications exist alongside others supported by more innovative technologies resulting not only from transformation processes, but also from the various mergers and acquisitions that have taken place recently in the Spanish financial sector. This complexity makes it difficult for institutions to maintain an adequate control environment and, therefore, makes them more vulnerable.

It is important to note that in order to carry out these digital transformation processes and have access to the technological innovations that can best contribute to their business, financial institutions complement their capacities by procuring external services, investing in start-ups and acquiring third-party products. They also participate in incubators[8] and accelerators[9] or cooperate in consortia.

For this reason, the resilience and cyber security of these third parties, particularly providers, has become a growing concern for authorities and institutions. In fact, some of these providers have come to form the backbone of the financial sector, at a level comparable to market infrastructures and systemic institutions. They are

6 According to the FSB, "BigTech firms are large technology companies with extensive established customer networks".

7 The FSB defines FinTech as "technologically enabled financial innovation 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".

8 Incubators offer early-stage entrepreneurs and start-ups a physical space with basic services such as telecommunications in which to set an innovative business idea in motion. They generally provide access to a network of contacts and to expert teams that provide advice for the project to materialise.

9 Accelerators accompany start-ups that are already operating (unlike incubators, which help early-stage start-ups and provide basic services). Accelerators help boost start-up growth, acting as mentors in business model definition, trade strategies and even fund raising.

therefore unique points of failure, since the incidents affecting them, including unintentional ones, may have an impact on the sector as a whole.

Less well-known niche providers and other third-party dependencies not duly identified, arising from successive sub-contracting along the outsourcing chain, must be added to the list of large providers commonly considered systemic.

Against this backdrop, the COVID-19 pandemic has acted as a catalyst, accelerating the digitalisation processes already in progress at financial institutions and further increasing their dependence on technology service providers.

First, institutions have been forced to expand their portfolio of remote financial services. This has increased the exposure of their customers to attacks. Thus, a very significant growth in phishing,[10] vishing[11] and website and mobile application impersonation, inter alia, has been observed. Although institutions have made, and continue to make, significant efforts to improve customer cyber security education, some customers remain highly vulnerable, particularly those not familiar with digital channels prior to the pandemic.

Second, high teleworking levels have brought about additional risks for institutions and their employees, including those arising from the deployment of new technological infrastructure and the swift implementation of collaborative work solutions, insufficiently securitised access to corporate systems from personal devices and home connection networks, and the handling of confidential data at employees' homes. All of this has generated an increase in the exposure of institutions to cyber threats, exacerbated as a result of the speed imposed by the circumstances, which sometimes led to laxer controls or security analyses in order to continue operating.

In addition, the sudden need to increase the capacity of their systems forced many institutions to acquire additional external services, making them more dependent on third parties, particularly on cloud service providers. This market is highly concentrated in a relatively small number of providers; therefore, any incident at any one of them may have an immediate impact on multiple customer institutions.

The combination of these factors has created a very attractive environment for cyber attackers, who have seized the opportunity. Thus, during the pandemic, the financial sector has been the primary victim of cyber attacks worldwide, second only to the health sector.[12]

---

10 Phishing attacks are those where the attacker tries to fraudulently obtain confidential information (passwords, bank details, etc.) from legitimate users, by supplanting the digital identity of a trustworthy institution.

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

12 See BIS (2021).

Although some studies suggest that the financial sector is one of the critical sectors best equipped to deal with cyber risks, in part owing to its high level of regulation and supervision, cyber resilience among its participants is uneven. Sometimes the security measures and controls implemented by institutions, particularly smaller ones, are not enough to manage the cyber risks which the pandemic has exacerbated. It is therefore no surprise that among the institutions that have seen the biggest rise in the number of incoming cyber attacks, credit cooperatives, payment institutions and insurance companies (which belong to sectors where many small institutions are concentrated) stand out.[13]

In addition to cyber attacks attributable to organised crime, which pursue an economic benefit, an increase has also been seen in geopolitically motivated cyber attacks, some of which have been very sophisticated and were aimed at different supply chain providers.

2.2 The financial system in the face of geopolitical tensions

Since we have historical records, the economic and financial scenario has been both a cause of conflict and an object of dispute. State security has always been multi-dimensional. Aside from military matters, social, political and economic and financial aspects (the latter two being our concern at hand) have been and continue to be of vital importance. In its role of channelling economic resources and acting as a driving force for the productive business sector, the financial system is an essential element for economic development. For this reason, in the field of geopolitics, the adversaries' financial sector has become a priority for the enemies of any State.

In recent decades cyberspace[14] has become another domain, to be added to the traditional land, sea, air and space domains, as a means for attacking and defending objectives. States are investing ever more resources in developing their capabilities in this field, on both the defensive and offensive fronts.

From the defensive perspective, cyber resilience and the protection of critical financial sector infrastructures are reflected in the national security strategies of a growing number of countries, including Spain.[15] The International Telecommunication Union, a specialised agency of the United Nations for ICT, which publishes a global cyber security index each year, classified Spain in its 2020 edition[16] as one of the countries with the greatest capacity in terms of cyber security and cyber resilience (ranking fourth), a reflection of its maturity in this sphere.

13 *Ibid.*

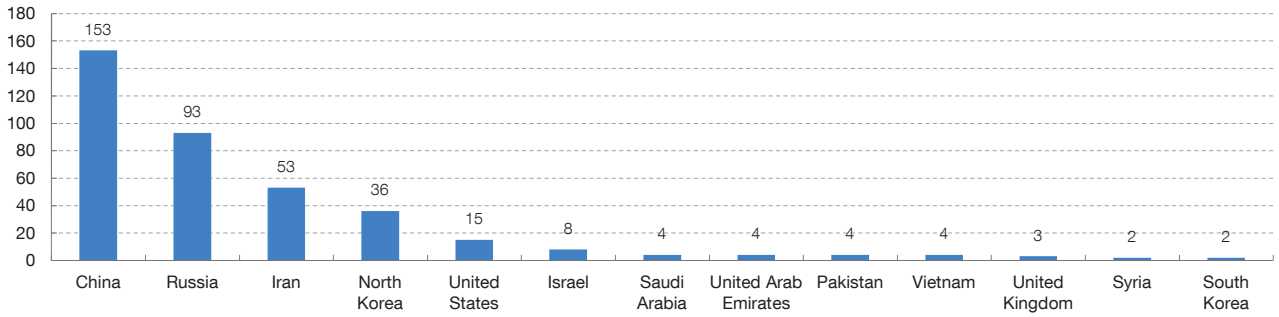
14 NIST defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

15 See DSN (2017 and 2019).

16 See International Telecommunication Union (2021).

Chart 1

ESTIMATION OF NUMBER OF STATE-SPONSORED CYBERATTACKS (2005-2020)



SOURCE: Council on Foreign Relations (2021).

As regards the offensive component, the organisation of specialised and operational groups responsible for launching attacks against other powers in cyber space is common, whether integrated in military structures or financed and organised outside them. Since 2005 at least 34 countries are suspected of having sponsored cyber attacks. As shown in Chart 1, it is estimated that China, Russia, Iran and North Korea sponsored 77% of all suspected operations[17] and that, in view of their resources and investment, they are expected to continue to be the most active actors in the future, although other western powers, such as the United States, the United Kingdom and Israel, also play a very significant role.

The term "state-sponsored actors" is generally used to refer to these types of State groups whose priorities, together with cyber espionage and influence operations, are cyber attacks against other States' critical infrastructures, with the financial sector having become a primary target. Thus, the 2019 Annual Report on National Security issued by Spain's National Security Department (DSN) indicates that in Spain 54% of cyber attacks against critical infrastructures targeted the financial sector.[18]

State groups have a high level of economic support, which enables them to have highly qualified staff and advanced offensive capabilities. Although their cyber attacks are comparatively less frequent, they have a potentially greater impact than campaigns conducted by non-state actors, such as hacktivists[19] or cyber criminals.

One of the main objectives of these groups is to destabilise the States they attack, and undermining confidence in the financial system is a very efficient way of

17 See Council on Foreign Relations (2021).

18 See DSN (2021).

19 Hacktivism (a combination of "hacking" and "activism"), also known as cyber activism, refers to the use of digital tools and attacks for politically motivated purposes.

achieving this. By taking advantage of the high degree of interconnectedness between the different participants in the financial sector, attackers seek to generate cyber incidents that can spread, escalate in magnitude and rapidly generate systemic consequences. In this connection, both the European Central Bank (ECB) and the European Systemic Risk Board (ESRB) have warned about the existence of plausible channels through which a cyber incident might evolve into a serious financial crisis.[20]

Given their nature, assets managed by financial institutions are easily (if not directly) monetisable and, accordingly, they are especially attractive for cyber attackers. Some of the most harmful State groups, such as those backed by North Korea, are particularly active in launching cyber attacks which aim to perform fraudulent transfers,[21] steal cryptocurrencies or demand ransom in exchange for returning to their victims and not disseminating the information encrypted by the attackers (ransomware).[22] The United Nations Security Council[23] recognises that these groups have become an additional source of financing for the States promoting them and a practical way of averting, or at least mitigating, the effect of international economic sanctions. Data theft is another channel used by attackers to obtain financing; cyber attacks financed by States with the aim of obtaining sensitive information that may be economically useful are increasingly frequent.

Lastly, as mentioned earlier, cyber attacks against third parties have become more numerous and sophisticated. The SolarWinds case is a paradigmatic example of the consequences of these attacks. In December 2020 it was discovered that software[24] distributed by SolarWinds had been modified by a group of cyber attackers to install a Trojan[25] in all the customers that used this product. The parties affected included numerous US federal agencies, NATO, the European Parliament and firms such as Microsoft, as well as others in various sectors, including the financial sector, around the world. This cyber attack, attributed to Russian intelligence services, which was extremely sophisticated and managed to go undetected for months, is a perfect example of the impact supply chain cyber attacks can have. Despite the time and resources needed to prepare and carry out such a far-reaching operation, the attackers managed to infiltrate thousands of organisations and important firms through a single point of entry, thereby multiplying manifold the attack's effectiveness and efficiency.

---

20 See ESRB (2020).

21 Attack on the Bangladesh Bank (the central bank of Bangladesh) in which fraudulent transfers were made via the SWIFT network totalling over $80 million.

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

23 See United Nations (2019).

24 The software, called "Orion", is used by customers to monitor their technological infrastructure.

25 In IT, a Trojan horse or Trojan is a programme that appears to be legitimate and harmless but, when executed, gives the attacker remote access to the infected computer.

3 Cyber resilience and the financial sector

3.1 Developments in cyber resilience in the financial sector

Although the use of the terms "resilience" and "cyber resilience" did not become widespread in the financial sector until 2016, this does not mean that before then there was no concern, both among the authorities and among the institutions themselves, for managing risks with a potential impact on institutions' resilience and, more specifically, on the technological front.

Back in 2005, concern for technological risk and business continuity, both within the broader field of operational risk management, had started to become widespread. The focus was mainly on technology and the authorities' perspective was microprudential. In this vein, in 2007 the Banco de España started to conduct the first on-site inspections to analyse the situation of technology and the management of associated risks at the institutions it supervised. For this purpose, it developed an initial methodology, which has been subsequently improved.

Since then, the concepts have evolved significantly, in parallel to the sector's growing digitalisation and awareness of the significance of these non-financial risks. For instance, the first version of the "Principles for the Sound Management of Operational Risk", published in 2011[26] by the BCBS, only mentioned the word "resilience" once and did not include any reference to the prefix "cyber". By contrast, the revisions to these principles published in 2021[27] mention "resilience" 22 times, use the prefix "cyber" eight times and include a new principle on ICT risk management.

In recent years it has become evident that cyber resilience is a global concern requiring the cooperation of all the actors involved. This has led to the emergence of numerous fora for debate and cooperation in the industry and among authorities, and to a highly significant regulatory and legislative effort. There has also been a shift towards a more holistic approach which does not focus exclusively on managing technology, but grants the same importance to persons and processes in organisations, linking up with existing disciplines, such as business continuity.

In 2014 the European Banking Authority (EBA) began to analyse the regulatory and supervisory status of technological risks in the different European jurisdictions. Since then, the EBA has created specialised working groups and published abundant regulations with much impact on the sector. Notable are the 2017 "Guidelines on ICT risk assessment under the Supervisory Review and Evaluation Process (SREP)",[28] the "Recommendations on outsourcing to cloud service providers", also published

26 See BCBS (2011).

27 See BCBS (2021b).

28 *EBA Guidelines on ICT risk assessment under the Supervisory Review and Evaluation Process (SREP) (EBA/GL/2017/05).*

in 2017[29] (subsequently integrated into the 2019 "Guidelines on outsourcing arrangements"[30] and repealed in their original form) and the 2019 "EBA Guidelines on ICT and security risk management".[31]

The Single Supervisory Mechanism (SSM) also commenced its activity in 2014, centred on the ECB as the banking supervisor for the euro area, and paid special attention to ICT risk from the beginning. Not only did it draw up ad hoc chapters in the supervisory manual for use during targeted on-site inspections, but it also developed a methodology for the ongoing assessment of ICT risk during the supervisory review and evaluation process. It also set up a procedure for institutions to report significant cyber incidents and carried out various horizontal analyses in connection with ICT risk and its management, part of whose findings are shared with the industry.[32]

The publication of "Guidance on cyber resilience for financial market infrastructures"[33] by CPMI-IOSCO[34] in 2016 and of the Bank of England's Discussion Paper "Building the UK Financial Sector's Operational Resilience"[35] in 2018 marked a turning point from which the discussion about operational resilience and cyber resilience started to become commonplace in the sector. The underlying idea is that implementing preventive measures to try to avoid cyber incidents is not sufficient. It is necessary to assume that they will occur and be prepared to manage them in order to minimise their impact and be able to continue providing critical functions and services.

Since 2018 all sorts of studies and regulations have been published on cyber resilience. Some notable examples include the publication in 2018 of the FSB's "Cyber Lexicon", the ECB's "Cyber Resilience Oversight Expectations"[36] and the BCBS's "Cyber-resilience: range of practices".[37] The BCBS also published in 2021 "Principles for Operational Resilience", which has aroused much interest in the sector.

Beyond the regulatory sphere, initiatives regarding the supervision of these risks have also grown significantly in recent years. Most authorities have allocated specialised resources both for ongoing monitoring and on-site inspections of institutions and for horizontal activities on the sector as a whole.

---

29 *Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).*

30 *Guidelines on outsourcing (EBA/GL/2019/02).*

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

32 See ECB (2021).

33 See CPMI-IOSCO (2016).

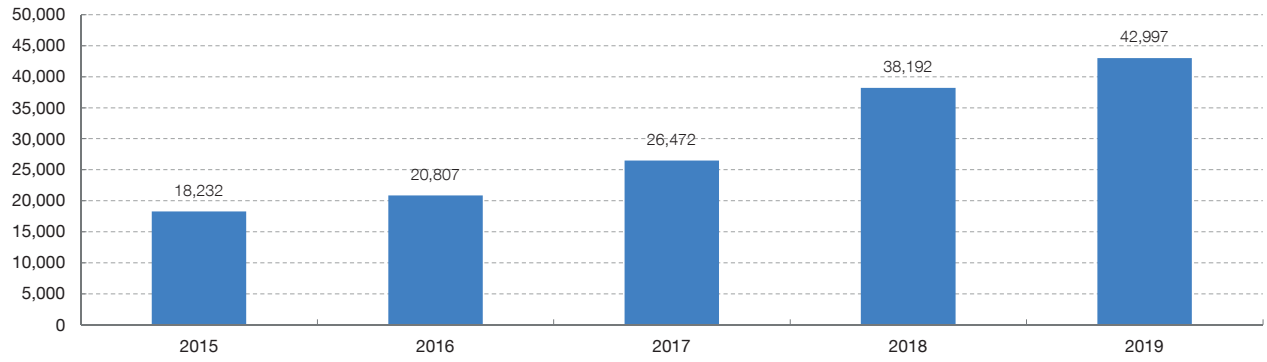
34 Committee on Payments and Market Infrastructures and International Organisation of Securities Commissions.

35 See Bank of England (2018).

36 See ECB (2018).

37 See BCBS (2018).

Chart 2
NUMBER OF INCIDENTS MANAGED BY THE CCN-CERT



SOURCE: Centro Criptológico Nacional (2020).

The Banco de España is one of the European supervisors with the greatest capacity and experience in this area. For this reason, it has contributed and continues to contribute significantly to the development of the main European and global regulatory and legislative initiatives and to the progress of the SSM's actions. From the perspective of market infrastructures, the Banco de España participates in the oversight of euro area payment systems and of central securities depositories, and in the supervisory colleges for central counterparties.

On the domestic front, in addition to exercising its supervisory and oversight responsibilities, it carries out numerous horizontal activities aimed at acquiring overall knowledge of Spanish institutions' technological situation and at improving their – and the overall financial sector's – cyber security and cyber resilience.

3.2 Current situation

As noted above, recent years have seen a substantial rise in the frequency and sophistication of attacks on the financial sector. Chart 2 shows the increase in the number of cyber incidents occurring in Spain and managed by the National Cryptology Centre (CCN),[38] a significant proportion of which targeted the financial sector. The CCN figures also show that 64% of the incidents managed in 2019 were classed at a high, very high or critical alert level.[39]

Accurately quantifying the costs associated with a cyber incident is no easy task since, while numerous studies have been conducted on the matter in recent years,

38 See CCN (2021).

39 In the report *Ciberamenazas y tendencias. Edición 2020,* incidents are classified into five alert levels: critical, very high, high, medium and low.

standard definitions and reliable, homogeneous and comparable historical data are as yet unavailable. There is nonetheless a consensus view that the fallout from cyber incidents (including the associated economic losses) is lessened at companies that have in place suitable measures to safeguard their systems and ensure any incidents are detected early, as well as response and recovery mechanisms to address such incidents.

The COVID-19 crisis (very long-lasting and global in reach) has underscored the pivotal role played by proper ICT management and the importance of cyber resilience for the correct functioning of the financial sector. Indeed, despite increased exposure to cyber incidents and the rise in the number of incoming cyber attacks, the impact on the sector has been limited. It is only fair to acknowledge that this is in large part thanks to the prior efforts and investments that both the authorities and market infrastructures, institutions and their providers (who have emerged as a key component of the ecosystem) have made in recent years in order to enhance their cyber resilience.

Key to achieving this goal is the proper management of all technological assets (everything from infrastructure items to data), through their entire life cycle: identification, classification in terms of criticality, changes required to ensure that assets remain operational in a diligent and secure manner, constant monitoring of their status and controlled elimination where they fall out of use.

Moreover, in response to an environment in which cyber threats are on the rise and attackers are ever more sophisticated, institutions have evolved from an approach centred on safeguarding their connections with the outside world (or perimeter) to a more holistic one, in which considering all potential threat vectors (including internal ones) is paramount. Thus, while continuing to work on perimeter security, they have now turned their attention to segmenting their internal networks or, in other words, to splitting them into isolated sub-networks. This is a crucial security mechanism since it prevents or hinders an attacker who compromises a system from gaining access to other systems outside the compromised sub-network.

As part of this holistic approach, which goes beyond technology and in which the human factor has a key role to play, training and raising the awareness of all of an institution's employees (and those of its providers) is crucial. The importance of these measures cannot be overstated, since employees are the weakest link in the chain and are often the entry vectors most targeted by attackers. With this in mind, institutions have in recent years been developing cyber security training programmes, both for their management and the rest of their staff, including courses and practical exercises, such as simulated phishing and vishing attacks.

As explained above, the concept of cyber resilience implies the capacity to anticipate, withstand, contain and rapidly recover from cyber incidents. Thus, it is important to

work on the assumption that cyber incidents are a given and that there may be disruptions to critical services, calling for recovery. Detection, response and recovery capacities thus take on particular importance, interlinking resilience with the field of business continuity.

With a view to guaranteeing the desired levels of cyber resilience, institutions set in place and trial their business continuity and IT contingency plans, envisaging an array of adverse scenarios, cyber attacks included. Moreover, they conduct crisis management simulations to check that suitable procedures are in place throughout the course of the incident simulated.

3.3 Trends

Rapid breakthroughs in technology and constant changes in the way such technology is deployed in the provision of financial services make up an ever-shifting backdrop, against which the threats and their materialisation in the various risks are also changeable. All of which leaves financial sector participants with no choice but to adapt constantly, as measures that are today effective to ensure the target levels of resilience may be found wanting tomorrow.

Specific cyber security-related measures and controls notwithstanding, institutions must give thought to the cyber security paradigm or model according to which they wish to integrate the implementation of such measures. With this in mind, government agencies such as the NSA[40] and organisations that lead the field in the technology space such as the NIST[41] have come out in favour of incorporating Zero Trust architectures, a model founded on the two premises detailed above: the assumption that, sooner or later, cyber incidents will occur, and the management of an ever more porous perimeter.

Up until a few years ago, the boundary between an institution and the world outside was clear-cut and easier to identify and manage. Today, those lines have been blurred owing to the multitude of connections required to enable remote access by employees and suppliers, the implementation of Bring Your Own Device[42] policies and the outsourcing of processes, e.g. to cloud service providers. Each of these new connections (as well as any assets connected to an institution's network) must be monitored and controlled.

The Zero Trust model advocates eliminating the principle of trust from all transactions. In other words, under this architecture, the aim is to segregate each IT asset (including

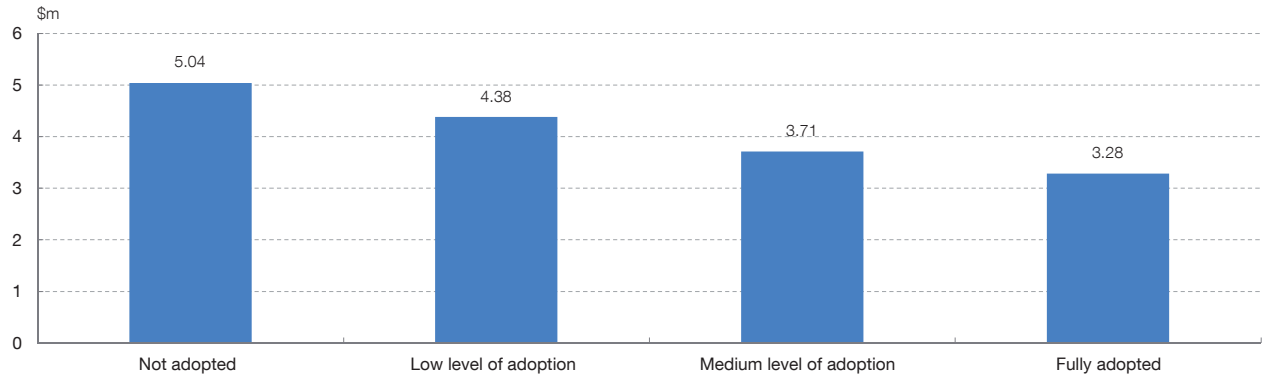
40 See NSA (2021).

41 See NIST (2020).

42 Bring Your Own Device, abbreviated to BYOD, is a corporate policy whereby employees take their own personal devices (laptops, tablets, mobiles, etc.) to their place of work in order to access company resources such as e-mail, databases and server files, as well as personal data and applications.

Chart 3

AVERAGE COST OF DATA BREACH BASED ON THE LEVEL OF ZERO TRUST DEPLOYMENT



SOURCE: IBM-Ponemon (2021).

data), and to apply the principles of least privilege and denial by default, thereby ensuring that users are at all times explicitly identified in every relevant transaction.

Thus, just as the importance of segregating networks has been stressed, making it harder for a successful attack to spread within an institution's internal network, this approach has now been broadened to include the segregation of all key assets and the performance of identity checks in any transaction that crosses any of the red lines drawn. Needless to say, once rolled out on a widespread basis, this model will enhance the security profile of an institution and reduce the impact of any cyber incidents, as can be seen in Chart 3. Yet it does have certain drawbacks, such as an increase in complexity and the transactional load, or a less user-friendly experience, so the implementation and application of the model calls for a detailed, risk-based study.

As for new technologies, the cyber resilience of financial institutions will be particularly affected by developments in artificial intelligence-related technologies. Here, use cases are identified in the fields of offensive and defensive cyber security, in what could be called a technology race.

On the offensive front, noteworthy examples include the use of artificial intelligence solutions to sidestep traditional access control mechanisms and, more effectively still, those based on images or voice patterns; inserting malware[43] in legitimate applications and controlling the use of such applications, or what has been dubbed smart malware, i.e. malicious software that learns an organisation's (users' or programs') permitted usage patterns, mimics them and capitalises on the existing vulnerabilities to escape unnoticed and propagate.

43 Malware refers to any type of software that intentionally performs harmful actions on an IT system without the user's knowledge.

Notable examples on the defensive side include the modelling of organisations' network traffic behaviour. Artificial intelligence enables the detection of particularly complex anomalous behaviour patterns in huge volumes of information, outperforming human analysts or traditional systems, integrating this within antivirus or intruder detection and prevention systems.

The end result of this race to harness the possibilities offered by artificial intelligence will in large part depend on which applications develop faster and on the pace of adoption by institutions.

Institutions will continue strengthening their recovery models since, in the last instance and assuming a cyber incident occurs, they will in certain adverse circumstances need to recover their services where the integrity, confidentiality or availability of their information has been affected. Of particular interest in this regard are data vaulting measures, a term that refers to the offline, offsite storage of the set of critical data an institution needs to ensure its critical services remain operational.

A case in point is the initiative currently in progress at Sheltered Harbor, a subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC), with the participation and backing of the leading US banking associations.[44] The operating model set in place requires participating institutions to send their information, encrypted and in the agreed format, to shared data vaulting facilities so that, in the event of a major contingency and thanks to their participation in the initiative, their data can be recovered and processed at the facilities of other participating institutions that have not been affected.

Meanwhile, the authorities continue stepping up their efforts in the area of resilience. Notable from a regulatory standpoint is the development of the Digital Operational Resilience Act (DORA), the European Commission's new legislative proposal for the financial sector. DORA will apply to financial institutions of all types and sizes, in a proportionate manner, and sets out requirements concerning the management of technology-related risks; the identification, classification and reporting to the authorities of significant cyber incidents; the conduct of cyber resilience tests and information-sharing. However, DORA does not merely standardise and tighten the requirements in terms of how financial institutions must manage cyber risk, it also sets in place a ground-breaking framework for the direct oversight of the technology providers deemed critical for Europe's financial sector. Expected to enter into force in 2024, this regulation constitutes a stringent, harmonised standard for financial institutions across the board, and will no doubt help to bolster the sector's resilience.

Elsewhere, authorities across many jurisdictions are working to encourage financial institutions and market infrastructures to conduct cyber security stress tests,

44 See the Sheltered Harbor website.

simulating sophisticated cyber attacks. With this in mind, the Banco de España is now rolling out TIBER-ES, the local adoption of the TIBER-EU cyber security testing framework, with the aim of shoring up the resilience of Spain's financial sector.

Aside from ensuring that institutions undergo such testing individually, it is also important to encourage sector-wide testing, with a view to enhancing coordination and reporting mechanisms to deal with events with a systemic impact. Notable here are the exercise programmes of the G7's Cyber Expert Group, the work of the European Systemic Cyber Group (ESCG) or the mandate to be given by DORA to European financial sector authorities to make further headway in this direction.

It is increasingly clear that, in cyber security more than any other area, cooperation is key. This has been taken on board by institutions, who share among themselves relevant information on cyber incidents and cyber threats (what is generally referred to as "cyber intelligence") in a range of fora organised by the industry, such as the FS-ISAC.[45] Examples of cooperation between institutions, the authorities and other financial system participants can also be found, such as the CIISI-EU (Cyber Information and Intelligence Sharing Initiative)[46] platform.

Meanwhile, the authorities are stepping up their cooperation, not only within the financial sector but also with other authorities on a range of cyber security-related matters, such as cyber incident response centres and intelligence agencies.

The role of the financial sector authorities has gradually changed in step with the increasing importance of technology and the goal of enhancing cyber resilience. It has shifted from an approach traditionally focused on the solvency and liquidity of institutions and the smooth running of critical financial functions to considering technology as all-important for the functioning of the sector and supervising its use and development, as well as the risks it entails. Indeed, the authorities are taking on an active role in the cyber resilience space, emerging as a key player in the management and coordination of potential cyber incident-related crises.

Nonetheless, when it comes to bolstering cyber resilience in the financial sector, financial institutions, market infrastructures and providers will continue to take centre stage. Following through on their efforts in this area, they will have to integrate their management of human and organisational factors with their own technological progress and the breakthroughs made in cyber security and business continuity if they wish to successfully address the foreseeable increase in the sophistication and impact of cyber attacks.

45 See the FS-ISAC website.

46 See the CIISI-EU website.

REFERENCES

Bank of England (2018). *Building the UK financial sector's operational resilience*, Bank of England and Financial Conduct Authority (FCA) Discussion Paper, July.

Bank for International Settlements (BIS) (2021). Covid-19 and cyber risk in the financial sector, *BIS Bulletin* No 37, January.

Basel Committee on Banking Supervision (BCBS) (2011). *Principles for the Sound Management of Operational Risk,* June.

Basel Committee on Banking Supervision (2014). *Cyber resilience in financial market infrastructures,* November.

Basel Committee on Banking Supervision (2018). *Cyber-resilience: Range of practices,* December.

Basel Committee on Banking Supervision (2012a) *Principles for Operational Resilience,* March.

Basel Committee on Banking Supervision (2012b). *Revisions to the Principles for the Sound Management of Operational Risk,* March.

Centro Criptológico Nacional (CCN) (2020). *Ciberamenazas y tendencias. Edición 2020,* CCN-CERT IA-13/20, September.

Council on Foreign Relations (2021). *Cyber Operations Tracker,* public database on state-sponsored incidents.

CPMI-IOSCO (2016). *Guidance on cyber resilience for financial market infrastructures,* June.

Departamento de Seguridad Nacional (DSN) (2017). *Estrategia de seguridad nacional.*

Departamento de Seguridad Nacional (2019). *Estrategia Nacional de Ciberseguridad.*

Departamento de Seguridad Nacional (2021). *Informe Anual de Seguridad Nacional 2020,* March.

European Banking Authority (EBA) (2019). *EBA Guidelines on ICT and security risk management,* November.

European Central Bank (ECB) (2018). *Cyber resilience oversight expectations for financial market infrastructures,* December.

European Central Bank (2021). *Annual report on the outcome of the 2020 SREP IT Risk Questionnaire - Feedback to the industry,* July.

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

Financial Stability Board (FSB) (2018). *Cyber Lexicon*, 12 November.

Hernández de Cos, P. (2019). "Financial technology: the 150-year revolution", keynote speech given as Chairman of the BCBS at the 22nd Euro Finance Week, Frankfurt, 19 November.

Herrera, F. J., J. Munera and P. Williams (2021). "Cyber risk as a threat to financial stability", *Financial Stability Review* No 40, Spring, Banco de España.

IBM-Ponemon (2021). *Cost of a Data Breach Report 2021*.

International Telecommunication Union (2021). *Global Cyber security Index 2020.*

National Institute of Standards and Technology (NIST) (2020). *Zero Trust Architecture*, NIST Special Publication 800-207, August.

National Security Agency (NSA) (2021). *Embracing a Zero Trust Security Model,* February.

United Nations (2019). *Final report of the Panel of Experts of the 1718 DPRK Sanctions Committee,* Security Council report on the Democratic People's Republic of Korea, 5 March.