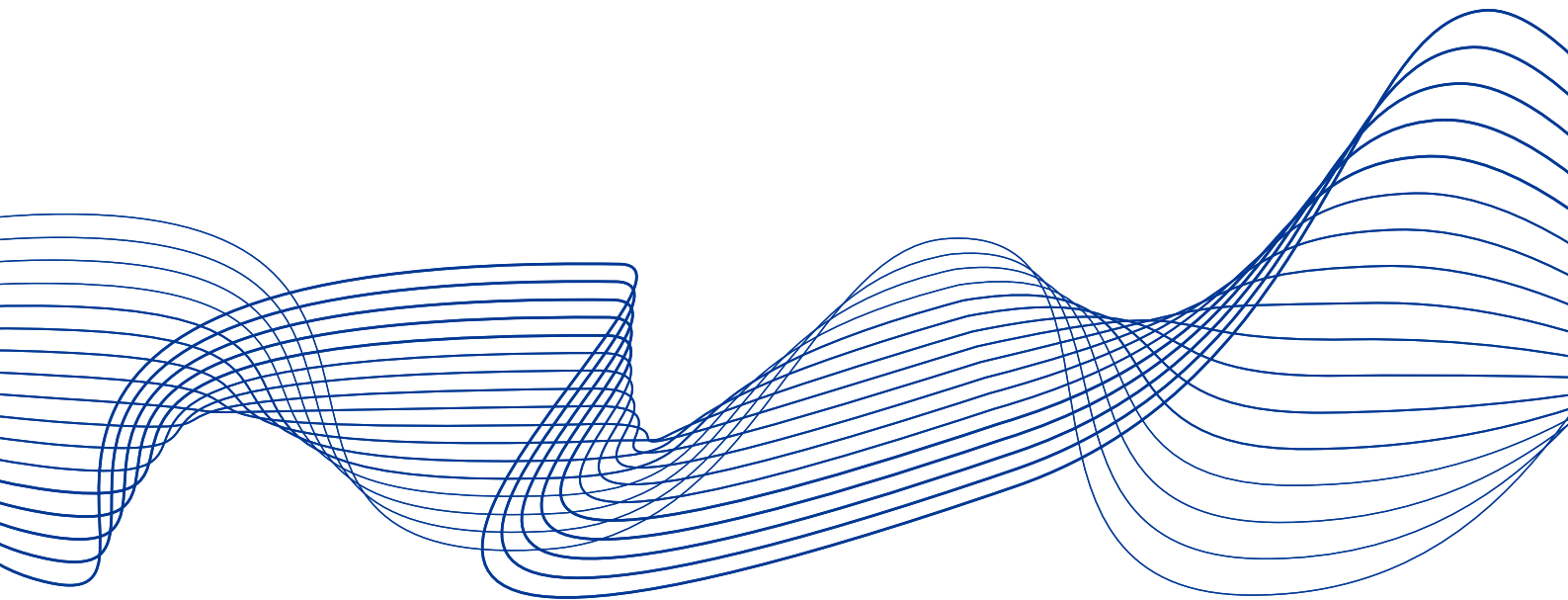


Systemic cyber risk

February 2020



ESRB

European Systemic Risk Board

European System of Financial Supervision

Contents

Executive summary	2
1 Introduction	5
2 Cyber risk	7
2.1 Overview	7
Box 1 Definitions related to cyber risk	9
2.2 Regulatory and industry initiatives	11
2.3 Recent cyber incidents	17
2.4 Common individual vulnerabilities across ESRB members	19
2.5 Financial stability and cyber risk	22
3 Can cyber risk become systemic?	24
3.1 Conceptual systemic cyber risk model	24
3.2 Scenario analysis	27
3.3 Grouping and prioritisation of common individual vulnerabilities	36
3.4 Main findings of the vulnerability analysis	37
4 Conclusions	40
4.1 Summary	40
4.2 Policy areas and potential options	41
Annex 1: Report on common individual cybersecurity vulnerabilities	44
Introduction	44
Identification of cyber vulnerabilities	46
Thematic grouping of cyber vulnerabilities	47
Annex 2: Overview of other relevant studies	52
References	54
Imprint and acknowledgements	55



Executive summary

During recent decades, the global financial system has become more digitalised and interconnected. For its functioning, the real economy requires the financial system to perform a range of key economic functions reliably. These include payment services, securities trading, settlement services and deposit taking, among others. These processes have become increasingly digitalised, creating new and important interdependencies. Hence, the financial system has come to rely critically on robust information and communications technology (ICT) infrastructures and the confidentiality, integrity and availability of data and systems. It follows that key economic functions can be disrupted through cyber incidents that affect the information systems and data of financial institutions and financial market infrastructures. Understanding the impact of such disruptions on financial stability is the focus of this report.

Cyber risk is characterised by three key features that, when combined, fundamentally differentiate it from other sources of operational risk: the speed and scale of its propagation as well as the potential intent of threat actors. The interconnectedness of various information systems enables cyber incidents to spread quickly and widely. Some recent incidents have demonstrated actors' ability to penetrate the networks of large organisations and incapacitate them quickly. Cyber incidents can also spread widely across sectors and beyond geographical borders, including to entities which are not the primary target or source of disruption. Malicious cyber incidents are becoming more persistent and prevalent, illustrating the high level of sophistication and coordination that threat actors are able to achieve.

The ESRB has developed an analytical framework to assess how cyber risk can become a source of systemic risk to the financial system. The four stages of this conceptual model (context, shock, amplification, systemic event) facilitate a systematic analysis of how a cyber incident can grow from operational disruption into a systemic crisis. In particular, the framework could assist in analysing systemic vulnerabilities that amplify the shock of a cyber incident, and in understanding at which point a cyber incident may become systemic. The ESRB also surveyed its membership to form a view on common individual vulnerabilities across ESRB jurisdictions. Combining these elements, the ESRB has considered a number of historical and hypothetical scenarios. It used these scenarios to try to understand the distinction between severe operational disruption to the financial system, on the one hand, and a systemic crisis, on the other hand.

A cyber incident can evolve into a systemic crisis when trust in the financial system is eroded. A critical point in assessing whether a cyber incident will progress to become a systemic financial crisis lies in the differentiation of whether or not the incident escalates from an operational level into the financial and confidence realms. In order for a cyber incident to raise systemic financial and confidence concerns, either the disruption to critical functions supporting the real economy or the generated (or anticipated) financial losses from the incident need to reach a level where the financial system is no longer able to absorb the shock. For instance, a perceived irrecoverable destruction, alteration or encryption of account balances of one or several financial institutions could constitute a sufficiently severe shock to the financial system. This could occur through operational disruption, financial losses and loss of confidence in the system, triggering



liquidity freezes, bank runs and panic. The loss of confidence in the integrity of data could in itself trigger similar reactions.

The ESRB's analysis illustrates how a cyber incident could, under certain circumstances, rapidly escalate from an operational outage to a liquidity crisis. In turn – and in common with historical financial crises – this liquidity crisis could, in certain circumstances, lead to a systemic crisis. This could happen, for example, when the size of anticipated losses is very large. Thus the later stages of a cyber crisis are similar to those seen in a more traditional financial crisis: large (expected) financial losses and a significant weakening of the trust in the financial system.

The ESRB has therefore identified cyber risk as a source of systemic risk to the financial system, which may have the potential for serious negative consequences for the real economy. From a macroprudential perspective, the ESRB considers the main shocks to be the destruction, encryption or alteration of data related to value. Such shocks could cause a cyber incident to develop into a systemic event, impairing the provision of key economic functions, generating significant financial losses and undermining confidence in the financial system.

Standard-setting bodies, national and international authorities, as well as industry groups, are combining their efforts to mitigate cyber risks. The Financial Stability Board (FSB) has developed a Cyber Lexicon to foster a common language and facilitate cross-jurisdictional communication on cyber risk. At the European Union (EU) level, the mandate for the European Network and Information Security Agency (ENISA) has been strengthened and the European Supervisory Authorities (the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA)) have issued guidelines on how their supervised entities should implement best practices in ICT risk management. Other legislation and frameworks (e.g. the Directive on Security of Network and Information Systems (NIS Directive), the Threat Intelligence-based Ethical Red Teaming (TIBER-EU) framework and the ECB's Cyber Incident Reporting) are addressing various aspects of cyber risk across a range of industries. The ECB has established the Euro Cyber Resilience Board, a market contact group bringing together regulators and financial market infrastructures. The G7 has started conducting cross-jurisdictional cyber exercises. These initiatives address different aspects of cyber risk and contribute to its mitigation.

To mitigate further the risk of a systemic cyber incident materialising, more work is required to address system vulnerabilities and reduce the potential for widespread disruption through amplification channels. The scenario analysis in this report reveals that the loss of confidence in the financial system plays a key role in a cyber incident developing into a systemic crisis. A number of policy areas therefore merit further exploration: First, given the speed and scale at which such a cyber incident may unfold, rapid coordination between stakeholders and a consistent and clear communication from authorities may be required in order to shore up confidence. Different ongoing work streams could be leveraged to achieve this goal. Second, effective restoration of key economic functions requires planning, including agreeing on a clear division of tasks between industry and authorities, and between (technical) incident management and (financial) consequence management. This may also include reflections on central bank emergency communications, interventions or assistance when a cyber crisis becomes a financial stability crisis. Finally, the cyber equivalent of capital buffers is preparedness and resilience. In that sense, the operationalisation of systemic resilience mechanisms such as data vaulting, among



other things, merits further exploration. This is of particular importance as many recovery and resolution plans are contingent on essential data being available or recoverable.

The ESRB intends to explore some of the potential systemic mitigants in future work. Taking stock of the findings in this report, the ESRB intends to leverage its broad institutional composition and network to evaluate the costs and benefits of different systemic mitigants going forward.



1 Introduction

Over the course of recent decades, cyber incidents have become more frequent as well as increasingly costly and damaging. Recent cyber incidents, such as the outages of card payment systems or Petya, NotPetya and WannaCry, have further demonstrated the potential for damage to software or operating systems to spread quickly and widely. Different groups of threat actors have also successfully carried out a number of cash-out malicious incidents targeting both commercial and central banks.¹ This trend is expected to continue, especially as sophisticated tools and methods previously only available to nation-states are now available to criminal actors at low or no cost.

The increasing digitalisation of financial services in combination with the presence of high-value assets and data make the financial system vulnerable to cyber incidents. The high level of interconnectedness across financial institutions, financial markets and financial market infrastructures, and particularly the interdependencies of their IT systems, constitute a potential vulnerability as a localised cyber incident could quickly spread across markets and jurisdictions. For example, a large proportion of payments and other financial infrastructure for trading, custodial services and online retail banking have become digitalised. The heavy reliance of these infrastructures on IT systems and electronic communication means, as well as the presence of legacy IT systems, have significantly increased the potential damaging impact that a cyber incident could have on the financial sector. Furthermore, the adoption of new technologies such as cloud computing creates new interdependencies with entities that may operate outside the boundaries of regulated financial systems. Whilst some aspects of these interdependencies contribute to greater resilience, they also present new risks.

In 2017, the ESRB established the European Systemic Cyber Group (ESCG) to form a view on systemic cyber risks in the EU. The ESCG's mandate requested the group to examine cybersecurity vulnerabilities and their potential impact on financial stability and the real economy. The group's mandate covered four elements: (i) to collate and examine common cybersecurity vulnerabilities identified by ESRB members across domestic supervised entities, and understand the methods used by each member to identify and assess these vulnerabilities; (ii) to compare how ESRB members form a view on system-wide vulnerabilities; (iii) to identify, prioritise and report on such common weaknesses across the ESRB membership; and (iv) to discuss relevant international work being undertaken in other fora to raise awareness and minimise the duplication of efforts.

In order to form a view on common individual vulnerabilities, the ESCG conducted a survey among the ESRB membership and developed an analytical framework to investigate whether and how cyber risk could create systemic risks for financial stability. The survey shed light on the most common individual vulnerabilities, while the conceptual model helped to understand under which circumstances a cyber shock could affect the financial system, develop into a systemic crisis, and create widespread disruption to the real economy.

¹ For instance, the cyber heists on Cosmos Bank in India in 2018 and on the central bank of Bangladesh in 2016.



The remainder of this report is structured as follows. Section 2 describes the broader cyber risk landscape by providing definitions, summarising initiatives by both the private sector and public authorities, and providing an overview of a number of notable recent cyber incidents. The section concludes with the results of a cyber survey conducted among the ESRB membership and describes the relationship between cyber risk and financial stability. Section 3 addresses the main question as to whether cyber risk can become systemic. To this end, the analytical framework developed by the ESCG is summarised in Section 3.1 and applied to both real and hypothetical scenarios in Section 3.2. The remainder of Section 3 categorises the identified vulnerabilities. Section 4 concludes with an overview of policy areas that may be worth exploring.



2 Cyber risk

2.1 Overview

The financial system performs a number of key economic functions which support the real economy. For the real economy to function properly, the financial system needs to perform a wide range of key economic functions reliably and robustly. These include the provision of services related to payment and settlement, wholesale funding, current and savings accounts, as well as derivatives and securities trading.² Table 1 provides a more granular overview of these economic functions. In the context of bank resolution and depending on the provider and the circumstances, some of these key economic functions can be viewed as “critical functions”, which are “activities, services or operations the discontinuance of which is likely in one or more Member States, to lead to the disruption of services that are essential to the real economy or to disrupt financial stability [...]”.³

During recent decades, the global financial system has become more digitalised and interconnected. In capital markets, since the late 1960s physical shares have gradually been replaced by electronic book-entry securities (dematerialisation); as of 2010 the majority of securities only exist, and are traded at a global level, in electronic form. On the retail side, during the last decades banks have reduced the number of branches and expanded their online banking services. More recently, peer-to-peer lending, e-money providers and other fintech companies have started offering their services via apps and web platforms. At the same time, many components of the financial market infrastructure (central clearing, payment and settlement services, central bank real-time gross settlement systems, etc.) have become fully digitalised.

The financial system relies on a robust ICT infrastructure in order to perform these key economic functions. Interconnected and interdependent ICT systems need to process data reliably so that the financial system can perform its key economic functions. Moreover, these systems rely on critical data, which need to be protected. Confidentiality,⁴ integrity⁵ and availability⁶, known as the “CIA triad”, are three crucial properties for the data processed by these ICT systems.⁷

² More specifically, the FSB views (i) deposit taking and savings, (ii) lending and loan servicing, (iii) capital markets and investment, (iv) wholesale funding markets and (v) payments, clearing, custody and settlement as five overarching categories of services that the financial system provides to the real economy: See **“Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services”**, FSB, July 2013.

³ See the **Single Resolution Board’s website**.

⁴ Defined by the FSB **Cyber Lexicon** as the property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.

⁵ Defined by the FSB Cyber Lexicon as the property of accuracy and completeness.

⁶ Defined by the FSB Cyber Lexicon as the property of being accessible and usable on demand by an authorised entity.

⁷ The ESCG has further identified authenticity, accountability, non-repudiation and reliability as important properties to be preserved by cybersecurity measures. For more details, see “The making of a cyber crash”, *ESRB Occasional Paper Series*, Forthcoming.



The databases and ICT processes that underlie the key economic functions can be disrupted in a number of ways.

Not all disruptions to databases and ICT processes are alike. In some instances, organisations experience disruptions which are the result of unplanned IT changes or user error or are the result of previously unknown weaknesses (e.g. flaws in operating systems or software). In other cases, disruption is the result of targeted and malicious activity, aimed at causing actual disruption of systems and/or undermining confidence in these systems or their underlying data. Cyber incidents can: (i) jeopardise the cybersecurity of an information system or the information the system processes, stores or transmits; or (ii) violate the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. When using the term “cyber risk”, the report refers to the combination of the probability of such events occurring and their impact.

Table 1

Key economic functions of the financial system

Economic functions	
Deposit taking and savings	Retail current accounts
	SME current accounts
	Retail savings accounts/time accounts
	SME savings accounts
	Corporate deposits
Lending and loan servicing	Retail mortgages
	Retail lending (secured/unsecured)
	Retail credit cards
	SME lending (secured)
	Corporate lending
	Trade finance
	Infrastructure lending
	Credit card merchant services
Capital markets and investment	Derivatives
	Trading portfolio
	Asset management
	General insurance
	Life insurance, pensions, investment and annuities
Wholesale funding markets	Securities financing
	Securities lending
Payments, clearing, custody and settlement	Payment services
	Settlement services
	Cash services
	Custody services
	Third-party operational services

Sources: FSB, Bank of England and ESRB.



The FSB has developed a set of definitions related to cyber risk to facilitate international discussions and coordination. The FSB definitions include both accidental and malicious cyber incidents. Box 1 elaborates on these definitions.

Box 1 Definitions related to cyber risk

In order to facilitate international coordination and communication, the FSB has developed a *Cyber Lexicon*⁸, which defines among other things the following cyber-related terms:

- **Cyber:** Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
- **Cyber event:** Any observable occurrence in an information system. Cyber events sometimes provide indication that a *cyber incident* is occurring.
- **Cyber incident:** A *cyber event* that:
 1. jeopardizes the *cyber security* of an information system or the information the system processes, stores or transmits; or
 2. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
- **Cyber resilience:** The ability of an organisation to continue to 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.
- **Cyber risk:** The combination of the probability of *cyber incidents* occurring and their impact.
- **Cyber security:** Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

The motives behind malicious cyber activity depend on the threat actor. While cybercriminals' primary goal is often to steal funds for private enrichment, other actors such as nation-states and terrorist groups may pursue more destructive objectives. The motives of the various threat actors can be broadly grouped into profit seeking (theft) and/or harm infliction (destruction of data and infrastructure, disruption of services). Table 2 provides examples of malicious activity by different threat actors along with their likely goals and motivation.

Accidental cyber incidents can have diverse sources. Ineffective change management processes can for instance result in misconfiguration incidents or inadequate system performance. Inappropriate monitoring processes as well as missing or insufficient communication within or among financial service providers can also lead to severe cyber incidents.

⁸ See "*Cyber Lexicon*", FSB, 12 November 2018.



This report focuses on cyber incidents originating from malicious activity, because they have the greatest potential to undermine confidence, but also reflects on the systemic impacts that could result from non-malicious cyber incidents.

Table 2

Cyber risk: threat actors, motivations and goals

Threat actor	Motivations	Goals	Examples
Nation-states, proxy groups	Geopolitical, ideological	Disruption, destruction, damage, theft, espionage, financial gain	Permanent data corruption Targeted physical damage Power grid disruption Payment system disruption Fraudulent transfers Espionage
Cybercriminals	Enrichment	Theft/financial gain	Cash theft Fraudulent transfers Credential theft
Terrorist groups, hacktivists, insider threats	Ideological, discontent	Disruption	Leaks, defamation Distributed Denial of Service (DDoS) attacks

Sources: ESRB, MI5 and Cambridge Centre for Risk Studies.

Cyber risk differs in significant ways from more traditional sources of risk such as credit, market, liquidity or operational risk. Credit, market and liquidity risk are normally revenue-driven risks that reflect an organisation's risk appetite. Operational risk encompasses the risk of financial losses stemming from inadequate or failed internal processes, people and systems or from external events, including legal risks but excluding reputational risks. Hence, cyber risk can be viewed as a subset of operational risk. It differs, however, in several material ways from more traditional sources of operational risks:⁹

- **Speed of propagation:** A cyber incident has the potential to crystallise and propagate throughout the system at a significantly quicker pace than other types of risk. During the 2017 NotPetya incident, major Ukrainian banks' systems were infected within less than a minute.¹⁰ It is in particular the interconnectedness of various automated information systems that enables cyber incidents to spread at such a fast pace. The speed of propagation, especially via automated tools, may be difficult to stop with traditional human intervention.
- **Scale of propagation:** A major cyber incident has the capacity to be more widespread in its impact than many other shocks, and is not constrained by geographical boundaries. The interdependence of the information systems supporting the financial system further enables cyber incidents to spread widely across sectors and beyond geographical borders, also to entities which are not the primary target or source of disruption. In 2018, the outage of Mastercard disrupted the ability to transfer and receive money using a credit card across

⁹ See also Kashyap and Wetherilt (2019).

¹⁰ See, for example, a [media report](#) on the event.

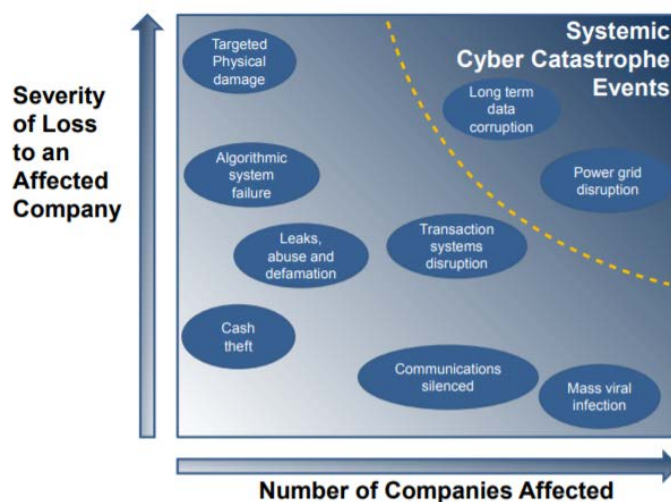


Europe. In 2017, the WannaCry incident spread across more than a hundred countries, infecting several hundred thousand computers, on a scale that was unprecedented.

- **Possible intent:** Some threat actors pursue a deliberate objective to cause major disruption to the financial system and the real economy. This stands in contrast to more traditional operational risk concepts often associated with accidental failures.

The degree of disruption experienced by organisations may vary depending on the nature of the incident and the number of companies affected. Figure 1 provides stylised examples of various cyber incidents in a two-dimensional plane, showing the number of entities affected (horizontal axis) and the severity of the loss for the affected companies (vertical axis). While a data leak or (potentially targeted) physical damage of infrastructure may be quite severe for the affected companies, the specificity of such an incident makes it unlikely that a large number of companies would be affected at the same time. By contrast, a long-term data corruption or the disruption/destruction of the power grid network would have very significant and widespread effects on the financial sector of a country or region. Additionally, the impact of (accidental) malfunctioning of IT infrastructure and processes can also vary depending on where this occurs along the value chain.

Figure 1
Scale and intensity of different cyber incidents



Source: Cambridge Centre for Risk Studies.

2.2 Regulatory and industry initiatives

This section reviews various (but not all) regulatory and industry efforts aimed at reducing cyber risk and provides an overview of initiatives by standard-setting bodies as well as regulatory authorities.



Cyber risk has become an important area of attention for international cooperation and standard-setting bodies. While the individual efforts of institutions to manage cyber risk have evolved in tandem with ICT developments, coordinated regulatory efforts have only taken place in more recent years. In addition, the borderless nature of cyber risk makes it particularly important for authorities to coordinate at an international level.

- In 2016, the **G7** noted that cyber risks were growing, with more diverse and frequent incidents, and published the *Fundamental Elements of Cybersecurity for the Financial Sector*, which serve as building blocks upon which entities can design and implement their cybersecurity framework.¹¹ In 2018 and 2019, two further sets of Fundamental Elements were published: the *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* and the *Fundamental Elements for Threat-led Penetration Testing*.
- In June 2016, the **Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO)** published their *Guidance on cyber resilience for financial market infrastructures*.
- In June 2019, the **IOSCO Cyber Task Force** published a report bringing together information from IOSCO member jurisdictions on their existing frameworks for cyber regulation¹² serving as guidance for good practices.
- In August 2017, the **Financial Stability Institute** published *Regulatory approaches to enhance banks' cyber security frameworks*, which reviews regulatory approaches in selected jurisdictions and draws some high-level policy conclusions, which may be helpful for banking supervisors when contemplating introducing or enhancing their cybersecurity banking regulations or supervisory tools.
- In November 2018, the **FSB** published the *Cyber Lexicon* to facilitate coordination and communication about cyber risks both within and across jurisdictions.¹³
- In December 2018, the **Basel Committee on Banking Supervision's Operational Resilience Working Group** published a report entitled *Cyber-resilience: Range of practices*, in which it describes and compares the range of regulatory and supervisory cyber-resilience practices on a cross-border basis.¹⁴
- Furthermore, the **International Association of Insurance Supervisors** has published an *Application Paper on Supervision of Insurer Cybersecurity*¹⁵, in which it provides standards and guidance to supervisors as regards their method for supervising cyber risk with a view to strengthening cyber resilience.

¹¹ For more details on the ongoing work of the FSB, see "**Cyber Incident Response and Recovery: Progress Report to the G20 Finance Ministers and Central Bank Governors meeting in Fukuoka, 8-9 June 2019**", dated 28 May 2019.

¹² See "**IOSCO Cyber Task Force – Final Report**", June 2019.

¹³ See "**Cyber Lexicon**", FSB, 12 November 2018.

¹⁴ See "**Cyber-resilience: Range of practices**", Basel Committee on Banking Supervision, December 2018.

¹⁵ See "**Application Paper on Supervision of Insurer Cybersecurity**", International Association of Insurance Supervisors, November 2018.



- The **International Organization for Standardization (ISO) and the International Electrotechnical Commission** developed and published standards¹⁶ on information security management systems to help financial institutions safeguard information assets such as financial information, intellectual property, employee details and information acquired through customers or third parties.

Cyber risk has also received attention from the European Supervisory Authorities (ESAs).

The ESAs have developed specific guidelines and expectations for ICT and security risk management of their supervised entities. In response to requests made by the **European Commission** in its 2018 FinTech Action Plan¹⁷, in April 2019 the ESAs published a *Joint Advice on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector*¹⁸ and a *Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector*¹⁹.

In 2019, the **European Banking Authority (EBA)** published its *Guidelines on ICT and security risk management*²⁰, which set out how financial institutions should manage their ICT and security risks. The guidelines also offer further clarity regarding supervisory expectations for the management and control of ICT risks. It is worth noting that in its August 2019 *Policy advice on the Basel III reforms: operational risk*²¹, the EBA highlighted the need for the Capital Requirements Regulation²² to be supplemented with articles or points that define ICT risk, using existing standards such as the FSB Cyber Lexicon.

In 2018, the **European Insurance and Occupational Pensions Authority (EIOPA)** published *Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies*²³. This report concluded that there is a need for a better understanding of cyber risk in order for the European cyber insurance market to develop further. Subsequently, EIOPA has engaged in a structured dialogue with insurers to foster the development of the cyber insurance market and address the main challenges for providing cyber insurance coverage and assessing cyber risk for underwriting purposes. In 2019, EIOPA published *draft Guidelines on outsourcing to cloud service providers*²⁴ and *draft Guidelines on information and communication technology (ICT) security and*

¹⁶ See the **ISO website**.

¹⁷ See “**FinTech Action Plan: For a more competitive and innovative European financial sector**”, Communication from the European Commission, 8 March 2018.

¹⁸ See “**Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector**”, 10 April 2019.

¹⁹ See “**Joint Advice of the European Supervisory Authorities to the European Commission on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector**”, 10 April 2019.

²⁰ See the **EBA’s website**.

²¹ See “**Policy advice on the Basel III reforms: operational risk**”, EBA, 2 August 2019.

²² **Regulation (EU) No 575/2013** of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

²³ See “**Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies**”, EIOPA, 2018.

²⁴ See “**Consultation on the proposal for Guidelines on outsourcing to cloud service providers**”, EIOPA, 2019.



*governance*²⁵ to provide clarification and enhance supervisory convergence regarding outsourcing to cloud service providers and regarding cyber security and governance respectively.

In February 2019, the **European Securities and Markets Authority (ESMA)** published its *2018 Annual Report and 2019 Work Programme*.²⁶ The latter sets out its plans to conduct a cybersecurity review of a subset of EU-registered credit rating agencies, with a view to gaining an understanding of their level of exposure to cybersecurity risk, considering also their implemented cybersecurity controls. Regarding trade repositories, ESMA intends to keep on liaising with the information security functions of the firms and other key personnel to ensure that the scope of work and the operations sufficiently cover the trade repositories' needs. Finally, ESMA will continue monitoring cybersecurity risk, as a subset of information security risk, as well as risks related to cloud computing within its ongoing supervision activities.

ECB Banking Supervision highlights the importance of banks' appropriate management of their IT and cyber risks. After the establishment of the **Single Supervisory Mechanism**, the ECB conducted thematic reviews on the topic in 2015, 2016 and 2017 to gain a more detailed understanding of the scope of the problem and has since established a cyber incident reporting process. As a result, the ECB has been collecting information from the banks it supervises on cyber incidents that have taken place, with the purpose of identifying and monitoring trends in this area. Moreover, the ECB conducts frequent on-site inspections with a focus on IT and cybersecurity.

Also, in 2016 the ECB published its *Stocktake of IT risk supervision practices*, which provides a picture of the IT risk landscape outside European banking supervision and focuses on the most important IT risk areas and leading IT supervisory practices.²⁷

The ECB's oversight function for financial market infrastructures (FMIs) highlights the need for FMIs to manage IT and cyber risks appropriately.

- In December 2018, the **ECB** published *Cyber resilience oversight expectations for financial market infrastructures*²⁸, which provide more detailed guidance on how to operationalise the above-mentioned CPMI-IOSCO Guidance. The report provides overseers with clear expectations to assess FMIs, which can serve as a basis for discussion between FMIs and their respective overseers.
- In May 2018, the ECB published *TIBER-EU*, a framework for *Threat Intelligence-based Ethical Red Teaming*.²⁹ This involves a "controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based

²⁵ See "**Consultation on the proposal for Guidelines on information and communication technology (ICT) security and governance**", EIOPA, 2019.

²⁶ See **ESMA's website**.

²⁷ See "**Stocktake of IT risk supervision practices – IT supervision outside European banking supervision**", ECB Banking Supervision, November 2016.

²⁸ See "**Cyber resilience oversight expectations for financial market infrastructures**", ECB, December 2018.

²⁹ See "**TIBER-EU framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming**", ECB, May 2018.



on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations".³⁰

- Finally, in 2018 the **Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)** was established. The ECRB aims to enhance the cyber resilience of FMI and critical service providers which are active in the EU on a cross-border basis, and of the wider EU financial sector by: (a) fostering trust and collaboration among pan-European FMI and critical service providers, on the one hand, and authorities, on the other hand; and (b) catalysing joint initiatives aiming to (i) increase the cyber-resilience capabilities of the financial sector, including joint solutions and awareness, and (ii) reinforcing the operational resilience of the financial sector generally.³¹

The financial industry has established a number of fora to share information and analysis on cyber risks. In 1999, the **Financial Services Information Sharing and Analysis Center (FS-ISAC)** was formed, which has since become the global financial industry's hub for sharing analysis and threat intelligence on cyber risks.³² The FS-ISAC is an industry consortium, which aims to reduce cyber risk in the global financial system by leveraging its intelligence platform, resiliency resources and a trusted peer-to-peer network of experts. It provides services to financial institutions which seek to mitigate and respond to cyber risks.

Looking beyond the financial sector, in recent years the EU has passed key legislation addressing various aspects of cyber risk. The Directive on Security of Network and Information Systems (NIS Directive), adopted in 2016, put in place requirements concerning national capabilities in the field of cybersecurity.³³ The NIS Directive established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for the economy and society, such as energy, transport, drinking water supply and distribution, banking, FMI, healthcare, digital infrastructure as well as key digital service providers.

The **European Union Agency for Cybersecurity (ENISA)**³⁴ has a key role in supporting the implementation of the aforementioned directive. In April 2019, the EU Cybersecurity Act strengthened the mandate of ENISA and laid the foundations for an EU certification framework for ICT digital products, services and processes.³⁵ ENISA's mission is to achieve "a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity". Furthermore, Directive

³⁰ See "**Cyber Lexicon**", FSB, 12 November 2018.

³¹ See the **ECB's website**.

³² See the **FS-ISAC website**.

³³ See **Directive (EU) 2016/1148** of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

³⁴ **Regulation (EC) No 460/2004** of the European Parliament and of the Council established ENISA with the purposes of contributing to the goals of ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. Regulation (EC) No 1007/2008 of the European Parliament and of the Council extended ENISA's mandate until March 2012. Regulation (EU) No 580/2011 of the European Parliament and of the Council further extended ENISA's mandate until 13 September 2013. Regulation (EU) No 526/2013 extended ENISA's mandate until 19 June 2020.

³⁵ See **Regulation (EU) 2019/881** of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).



2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems provides minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and provides for operational measures to improve cooperation among authorities on a cross-border basis.

Other legal acts such as the General Data Protection Regulation³⁶, as well as the Directive on privacy and electronic communications³⁷ and the Directive establishing the European Electronic Communications Code³⁸, also contribute to a high level of cybersecurity in the digital single market. Cybersecurity is also relevant for the scope of application of other EU legal acts with relevance to the financial market such as the Payment Services Directive 2 (PSD2)³⁹, the European Market Infrastructure Regulation (EMIR)⁴⁰, the Credit Rating Agency Regulation (CRAR)⁴¹, the Markets in Financial Instruments Regulation (MiFIR)⁴², the Markets in Financial Instruments Directive (MiFID)⁴³ as well as the Central Securities Depository Regulation (CSDR)⁴⁴. These legal acts consider technological innovation and lay out bespoke cybersecurity requirements. They may require further updating in the future, as the cyber risk landscape evolves.

To protect the Union's institutions and bodies, the EU has established a Computer Emergency Response Team for its institutions, bodies and agencies and an EU-wide Network of Computer Security Incident Response Teams. As part of the EU's commitment to a reinforced and high-level EU Networking and Information Security Policy, a **Computer Emergency Response Team (CERT-EU)** was established in 2012. Its mission is to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies by (i) helping to prevent, detect, mitigate and respond to cyber incidents and (ii) acting as the cybersecurity information exchange and incident response coordination hub.⁴⁵ The scope of CERT-EU's activities covers prevention, detection, response and recovery.⁴⁶ Moreover, the NIS Directive established the Computer Security

³⁶ See [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

³⁷ See [Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

³⁸ See [Directive \(EU\) 2018/1972](#) of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

³⁹ See [EBA Guidelines GL/2017/17](#) on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2).

⁴⁰ See [Regulation \(EU\) No 648/2012](#) of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.

⁴¹ See [Regulation \(EC\) No 1060/2009](#) of the European Parliament and of the Council of 16 September 2009 on credit rating agencies.

⁴² See [Regulation \(EU\) No 600/2014](#) of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012.

⁴³ See [Directive 2014/65/EU](#) of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

⁴⁴ See [Regulation \(EU\) No 909/2014](#) of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.

⁴⁵ See the [Arrangement](#) between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU).

⁴⁶ See the [CERT-EU website](#).



Incident Response Teams Network (CSIRTs Network). This brings together EU Member States' appointed CSIRTs and CERT-EU. It aims to contribute to developing confidence and trust between Member States and to promote swift and effective operational cooperation. The European Commission participates in the network as an observer. ENISA is tasked with actively supporting the CSIRT cooperation, providing the secretariat and supporting incident coordination upon request.⁴⁷

EU intelligence services are also engaged in the prevention and mitigation of cyber risks and cybercrime. In 2013, Europol set up the **European Cybercrime Centre (EC3)** "to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime". EC3 publishes the annual *Internet Organised Crime Threat Assessment* (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime. The IOCTA demonstrates how wide and varied cybercrime is and how EC3 is a key part of Europol's and the EU's response⁴⁸ through the use of forensics, strategy and operations. In 2010, Europol together with the European Commission and EU Member States established the **European Union Cybercrime Task Force (EUCTF)**⁴⁹, which comprises the heads of the national cybercrime units from the various Member States and representatives from Europol, the European Commission and Eurojust. The EUCTF's mission is to develop and promote a harmonised approach within the European Union to the criminal misuse of ICT and the fight against cybercrime. Other key actors involved in responding to cybersecurity crises include the EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (Sitroom), which are working together as the Single Intelligence Analysis Capacity (SIAC), and the EU Hybrid Fusion Cell based in the European Union Intelligence and Situation Centre (INTCEN).⁵⁰

2.3 Recent cyber incidents

In recent years, the frequency and impact of cyber incidents have increased; some malicious cyber incidents have become more sophisticated.⁵¹ In particular, there has been a significant increase in supply chain incidents and the use of targeted destructive malware⁵² and malicious cyber incidents are also becoming increasingly political in nature (nation-state sponsored).⁵³ At the same time, there have been a number of accidental incidents that have led to (temporary) unavailability of key economic functions.⁵⁴ This section provides a brief overview of recent cyber incidents and their relevance for the financial sector.

⁴⁷ See Article 12 of the **NIS Directive**.

⁴⁸ See the **Europol website**.

⁴⁹ See the **Europol website**.

⁵⁰ See Recital 15 of **Commission Recommendation (EU) 2017/1584** of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

⁵¹ See "**ACSC Threat Report 2016**", Cambridge Centre for Risk Studies "**Cyber Risk Outlook 2018**" and "**Cyber Risk Outlook 2019**", and Annex A of the "**CyRiM Report 2019**".

⁵² A **report** by Symantec notes that supply chain attacks are up by 78%, and destructive malware up by 25%.

⁵³ See "**Symantec Internet Security Threat Report**", Vol. 24, February 2019, Cambridge Centre for Risk Studies "**Cyber Risk Outlook 2019**" and "**ENISA Threat Landscape Report 2018**".

⁵⁴ See, for instance, Menze, T., "**The state of industrial cybersecurity**", July 2019.



The financial sector has traditionally been a key target for cybercriminals looking for financial gain. The Carnegie Endowment for International Peace in collaboration with BAE systems maintains an up-to-date database of significant malicious cyber incidents affecting the financial sector.⁵⁵ Notable examples of recent cyber incidents include:

- The hacking of the central bank of Bangladesh's SWIFT payment terminal in 2016, leading to fraudulent payment messages and USD 81 million being stolen (financial theft).
- The hacking of Cosmos Bank's ATM (automated teller machine) server in India in 2018, resulting in USD 13.5 million being stolen through fraudulent credit and debit card transactions (financial theft).
- The Banco de Chile's network incident, resulting in a USD 10 million loss (financial theft).
- The incident affecting the Banco de Mexico's domestic interbank payment system, SPEI, resulting in a USD 15 million loss (financial theft).
- The data breach at Equifax in 2017, resulting in an estimated 143 million US records containing customer information being stolen by hackers. This included social security numbers, dates of birth and credit card details (data breach/theft).

In 2017, the WannaCry and NotPetya cyber incidents, which originated outside the financial system, caused significant disruption across several countries and industrial sectors, with an impact on critical infrastructure and public services. These examples are covered in more detail in Sections 3.2.1 and 3.2.2.

While the total costs of cyber incidents are notoriously hard to establish, industry estimates range from USD 45 billion to USD 654 billion for the global economy in 2018.^{56 57} Accenture estimates the average cost of cyber incidents per company to have been around USD 13 million in 2018, an increase of 12% compared with 2017 and up 72% in the last five years. Estimating the total costs of cyber incidents is extremely difficult for two reasons. First, not all cyber incidents and losses are currently being reported. Second, even when an incident is reported, it is often not clear to what extent the loss estimate includes direct losses (loss of revenue, funds stolen, repair costs, etc.) as well as indirect losses (loss of reputation, damage to brand value, legal costs and fines, etc.).

Accidental failures of card service providers or bank backup systems have recently affected millions of customers globally. Such incidents remind us of the potential damage a cyber incident could cause in the financial sector, if it were to hit critical economic functions. Visa and Mastercard are key card service operators serving numerous banks and customers across the globe. Consequently, the impact of their accidental failures in summer 2018 quickly became a cross-border issue. The failure of hardware at Visa led to a partial outage lasting around eight

⁵⁵ See the [website of the Carnegie Endowment for International Peace](#).

⁵⁶ See the Online Trust Alliance's "[2018 Cyber Incidents and Breach Trends Report](#)".

⁵⁷ See ForgeRock's "[U.S. Consumer Data Breach Report 2019](#)". The White House also estimated the costs of malicious malware at between USD 57 billion and USD 109 billion (see "[The Cost of Malicious Cyber Activity to the U.S. Economy](#)", The Council of Economic Advisors, February 2018).



hours and affecting 5.2 million card transactions across Europe.⁵⁸ The outage of Mastercard a few weeks later affected customers globally.⁵⁹ Further notable examples of accidental failures include:

- In February 2019, the CME Group stopped trading for several global financial instruments such as S&P 500 futures and US Treasury futures due to technical problems. The outage had an impact on several markets and asset classes, including oil, natural gas and metals.⁶⁰
- A European bank experienced a severe storage failure disrupting several core services. After switching to the backup site, the bank discovered that the backups were not fully up to date, which created data inconsistencies. At this point the bank decided to halt all operations until the inconsistencies had been corrected. The incident was resolved within less than 48 hours.
- In June 2016, several media outlets reported that the payments of all customers of a major European bank had been booked twice due to a technical glitch. As the incident happened at the beginning of the month, the double booking concerned payments of rent, insurance premiums and electricity. Numerous clients were not able to perform further payments as their balances had become negative.

In sum, with the increasing role of malicious malware and state-sponsored activity, more disruptive cyber incidents therefore seem to be a question of “when” rather than “if”. Section 3.3 discusses these events in the context of the conceptual systemic cyber risk model in further detail.

2.4 Common individual vulnerabilities across ESRB members

In 2018, the ESCG surveyed ESRB member institutions to gather information on common individual vulnerabilities (CIVs) relevant for cyber risk. The questionnaire was based on thematic vulnerabilities that ESCG members had previously identified and agreed on. The group collected findings from cybersecurity assessments undertaken by 14 ESRB members across supervised/overseen entities (including banks, FMI and insurers).⁶¹ This led to the identification of the set of CIVs listed in Table 3. It is possible to group these vulnerabilities into different categories according to their nature: a gap (*target quality not present*), a weakness (*inadequate quality*), a susceptibility (*can be affected by something else*), and a flaw (*defect or imperfection*). These vulnerabilities can either arise in a *process* or be part of a *control measure*. Annex 1 provides a more detailed description of each of these vulnerabilities.

⁵⁸ See the June 2018 [article](#) in The Guardian.

⁵⁹ See the July 2018 [article](#) in the Financial Times.

⁶⁰ See the February 2019 [article](#) on the CNBC website.

⁶¹ The competent authorities of Belgium, Germany, Hungary, Ireland, Italy, Lithuania, Malta, The Netherlands, Poland, Romania, Slovenia, Spain, Sweden and the United Kingdom responded to the questionnaire.



Table 3

Common individual vulnerabilities identified across ESRB member jurisdictions

Common individual vulnerability (CIV)	Category
Insufficient industry oversight of third party suppliers and supply-chain	Weakness in process
Inadequate cyber hygiene	Weakness in process
Ineffective testing of people, processes and technology	Flaw in process
Insufficient cyber strategic planning and board level influence on cyber resilience	Weakness in process
Lack of investment in cyber threat intelligence	Gap in process
Presence of end of life systems	Susceptibility/flaw in asset
Technology centric focus underestimating responsibility of people and processes	Weakness in process
Organisational culture change needed for secure cybersecurity behaviours	Gap in process
Cyber undermines existing operational resilience arrangements	Weakness in control measures
High risk internet use requires better controls	Weakness in control measures
Firm scale and resources impact effective cyber risk management	Susceptibility in process
Insufficient credible third line of defence challenge in firms	Weakness in process
Cyber maturity targets not defined	Gap in process

Source: ESRB (ESCG).

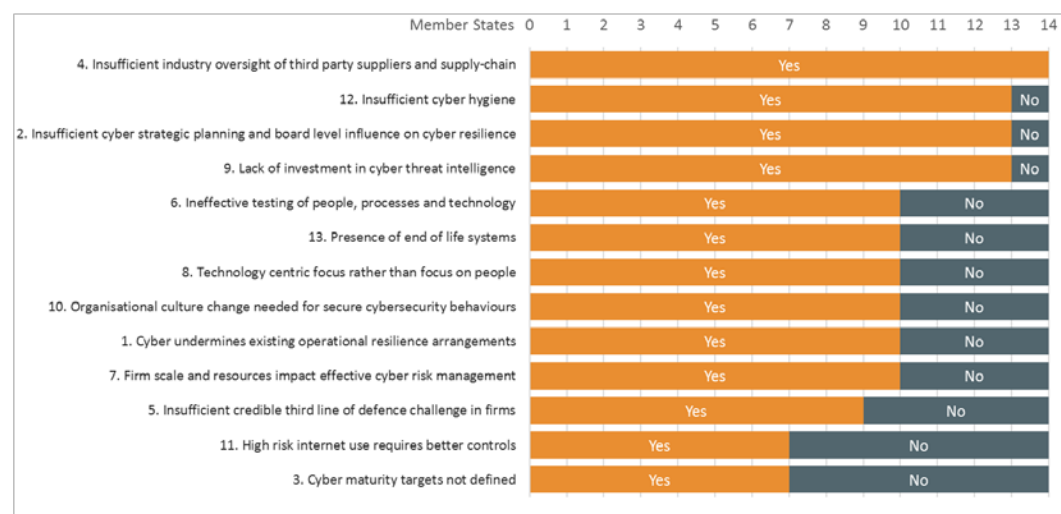
The survey showed that some vulnerabilities are more prevalent across member jurisdictions than others.

By their very nature, all 13 findings are relevant, as they indicate weaknesses in individual firms' approaches to cybersecurity. However, the survey revealed differences in the frequency of occurrence of the 13 vulnerabilities across the 14 responding member jurisdictions (see Chart 1). For instance, all 14 jurisdictions assessed that insufficient industry oversight of third-party suppliers and the supply chain was a vulnerability in their jurisdiction. But only half of the jurisdictions reported cyber maturity targets not being defined as a vulnerability.



Chart 1

Prevalence of each of the common individual vulnerabilities



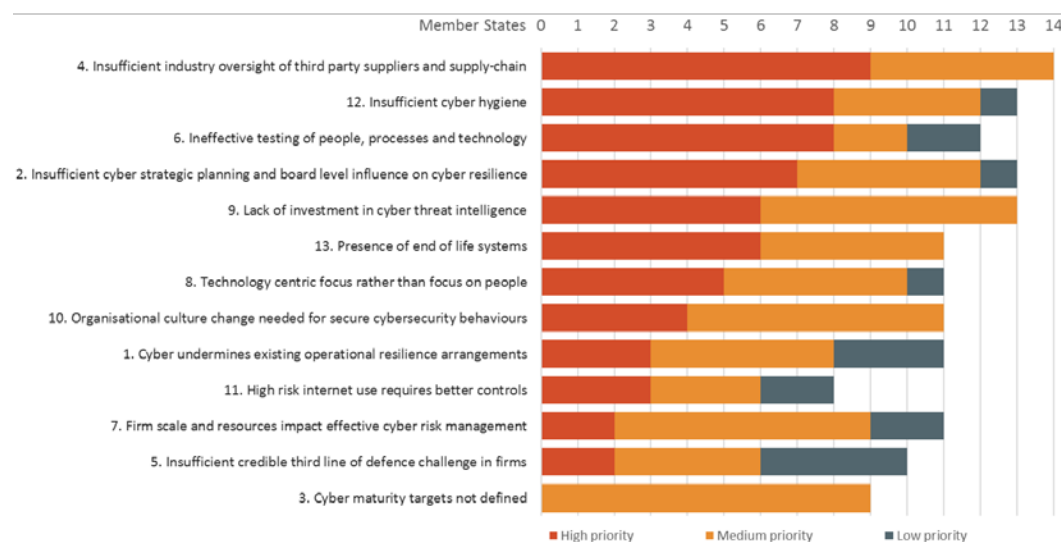
Source: ESRB (ESCG).

Members were asked to rank the vulnerabilities as high, medium or low priority in their jurisdiction.

Chart 2 illustrates the prioritisation of vulnerabilities provided by members. The survey revealed that the three highest-priority vulnerabilities were: (i) insufficient industry oversight of third-party suppliers and the supply chain; (ii) inadequate cyber hygiene; and (iii) ineffective testing of people, processes and technology.

Chart 2

Supervisory prioritisation rating of each of the common individual vulnerabilities



Source: ESRB (ESCG).



While individual institutions should have strong incentives to mitigate these vulnerabilities, these may not be sufficient or fully aligned with public interests. For example, institutions may not allocate sufficient resources to cybersecurity and instead allocate resources to more “visible” areas (i.e. focusing on profits and growth) at the expense of preparing for operational disruptions. Fearing reputational impacts, institutions may also be hesitant to share information with other entities after they have suffered a cyber incident, thus reducing opportunities to improve the management of existing vulnerabilities.

2.5 Financial stability and cyber risk

Having considered the cyber risks affecting individual firms and the extent to which there are common vulnerabilities across firms, this section considers the broader issue of financial stability.

“Systemic risk” means a risk of disruption in the financial system with the potential to have serious negative consequences for the internal market and the real economy.⁶² Financial stability in general refers to the proper functioning of financial markets in support of the real economy, i.e. their capacity to absorb shocks, continue providing the key economic functions such as facilitating payments, ensuring healthy lending markets and credit provision, transferring and transforming risk through intermediation and providing liquidity and price discovery mechanisms.⁶³ Financial stability is threatened when shocks cannot be absorbed and amplifying dynamics such as bank runs, liquidity and lending freezes, fire sales, market crashes or hyperinflation occur. Such dynamics, some of which are seen during severe crises, have the potential to lead to negative consequences for the real economy and can trigger severe recessions or depressions.

Beyond the magnitude of financial losses, uncertainty and the loss of confidence are critical catalysts in triggering financial instability. The evidence from historical financial crises demonstrates that financial instability – and the consequent loss of economic activity – could arise both as a result of direct actions by financial market participants in response to a given shock (e.g. the insolvency of a major bank) or of a broad fall in market or public confidence, which in turn causes financial market participants to modify their behaviour (e.g. a bank run or liquidity run). Thus, when considering the potential for a cyber shock to affect financial stability, it is important to consider both direct and indirect transmission channels.

Furthermore, the evidence from previous financial crises also tells us that both the size and the distribution of the initial shock matter, as well as whether there is a sufficient degree of transparency about the losses. In the absence of such information, financial market participants may become concerned about the ability of others to bear the losses and may withdraw funds, in turn creating further market instability. Hence, in the context of systemic cyber risk, it is important to understand the nature of the initial incident and the resulting financial losses.

⁶² See [Regulation \(EU\) No 1092/2010](#) of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board.

⁶³ See the [ECB's website](#).



Not every cyber incident represents a threat to financial stability. At the same time, it is not inconceivable that in future, a large-scale cyber incident in the financial sector could create disruption on such a scale that it has the potential to have serious negative consequences for the internal market and the real economy. The next section considers under what conditions a cyber incident could become a systemic event.



3 Can cyber risk become systemic?

This section summarises the conceptual model developed by the ESRB's European Systemic Cyber Group (ESCG) to analyse cyber risk. As noted in Section 2, to date no cyber incidents with a systemic impact for the financial system have materialised. It is important, however, to consider whether cyber risk has the potential to trigger serious and systemic financial repercussions, and how this might happen. To address this question, the ESCG has developed a conceptual model⁶⁴ to:

1. illustrate how the materialisation of cyber risk can trigger a systemic financial crisis;
2. improve our understanding of which vulnerabilities and factors need to be in place in order for a cyber incident to trigger a systemic crisis;
3. help authorities to analyse how cyber risks could develop in their jurisdiction into a systemic event; and
4. identify which common individual vulnerabilities (identified in the survey of the ESRB membership) have the greatest potential to trigger a systemic crisis, and therefore need specific regulatory attention.

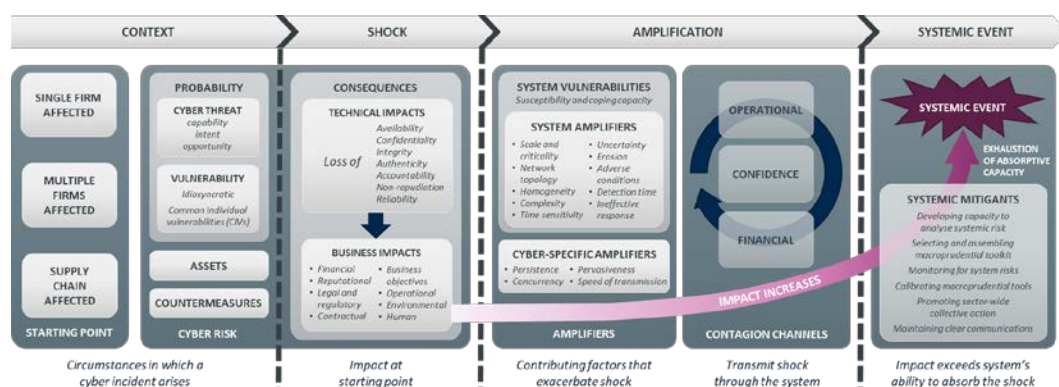
3.1 Conceptual systemic cyber risk model

The conceptual model splits the analysis of a cyber incident into four distinct phases: (i) context; (ii) shock; (iii) amplification; and (iv) systemic event. The phases are inspired by the FSB's approach to the macro-financial implications of operational and cyber risk, which decomposes the analysis of a cyber incident into general background and setting, the initial impact at source, its amplification through the system, and the final outcome (see Figure 2). Each phase is described in more detail in the following subsections.

⁶⁴ The conceptual model is described in detail in "The making of a cyber crash", *ESRB Occasional Paper Series*, Forthcoming.



Figure 2
Overview of the conceptual systemic cyber risk model



Source: "The making of a cyber crash", ESRB Occasional Paper Series, Forthcoming.

3.1.1 The context phase

The context phase describes the circumstances under which a cyber incident arises, in the form of a crystallised cyber risk. This phase examines the constituent parts of cyber risk which provide the setting and origin for a potential cyber incident, including:

- **cyber threats:** understanding the nature, localisation and motivation, if the act is deliberate, and the capability, intent and opportunities associated with the threat;
- **vulnerabilities:** distinguishing between idiosyncratic⁶⁵ and common individual vulnerabilities⁶⁶, to which other characteristics can be assigned to allow for ranking and categorisation;
- **assets:** classified by type, and expressed as "stores of value", i.e. a form of capital which can be saved, retrieved or exchanged at a later time; also includes non-financial assets such as hardware, software, intellectual property, etc.; understanding which cyber incidents have the potential to put value at risk;
- **countermeasures:** the methods which organisations can implement to mitigate cyber risk; and
- **starting point:** the three generalised entry points into the conceptual model, whereby a cyber incident hits either a single institution or multiple institutions simultaneously, or occurs via the supply chain.

⁶⁵ Individual vulnerabilities with unique characteristics for each individual entity.

⁶⁶ Prevalent occurrence of the same or similar vulnerabilities with shared characteristics across a system.



3.1.2 The shock phase

The shock phase describes the immediate technical and business impacts experienced at the point where the cyber incident has its initial impact. This stage focuses on the impact or consequences (as opposed to the likelihood of the shock). The conceptual model further distinguishes between technical and business impacts, thereby capturing the link between the loss of cybersecurity properties for the assets affected and the first-order effects of this disruption for the affected institution(s). In keeping with the Cyber Lexicon's definitions, the model illustrates the loss of one or more cybersecurity properties. It suggests that analysis should go beyond the traditional CIA triad (see the above-mentioned Occasional Paper, Figure 2.1).

Traditional business impact analysis (BIA) techniques are used to describe the non-technical aspects of localised disruption, and show how these feed into the transmission channels described in the later stages of the conceptual model (see Section 3.1.3). To help institutions and authorities use the shock phase, we provide an overview of impact measurement, and potential impact indicators (qualitative and quantitative) which approximate the impact over short, medium and long-term horizons.

3.1.3 The amplification phase

The amplification phase explores the interactions between the affected institutions and the systems which they use, and the factors that influence how shocks propagate through these systems. In this phase, the conceptual model brings together two concepts: (i) amplifiers, which if present are likely to increase the probability or consequences of the shock; and (ii) contagion channels, which transmit the shock through the systems.

The amplifiers are split into two types: system amplifiers or susceptibilities which may exacerbate any operational disruption, and cyber-specific amplifiers which relate to the unique features of cyber incidents. In isolation, each amplifier may not lead to a systemic outcome. However, if a rare alignment of amplifiers were to occur, the possibility of a systemic event greatly increases. For the transmission of the shock, the conceptual model describes three distinct channels – operational, confidence and financial – which can interact with each other concurrently and on a many-to-many basis.

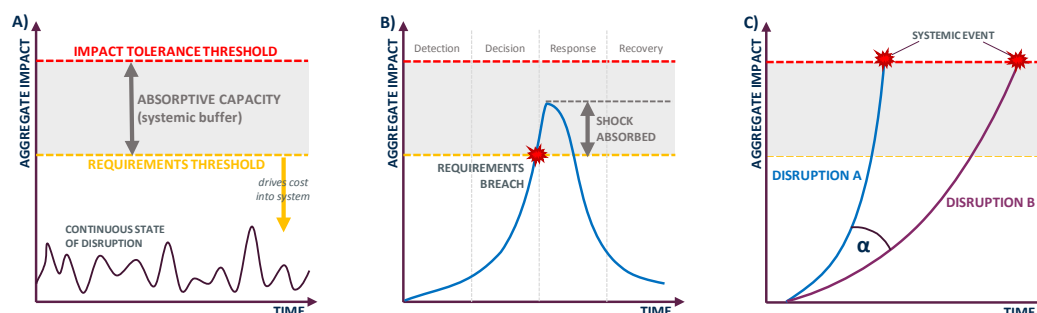
3.1.4 The systemic event phase

The systemic event phase examines the point at which the system is no longer able to absorb the shock. To be able to assess whether a systemic event can occur, it is first necessary to define the upper bound for that system, referred to in the conceptual model as the “impact tolerance threshold”. As with other systemic buffers, a second lower bound threshold is also defined, with the gap representing the absorptive capacity within the system (see Chart 3 below).



Chart 3

Three charts illustrating the concept of impact tolerance and absorptive capacity (A), a shock being absorbed (B), and disruptions with differing rates of impact amplification (C)



Source: Inspired by Bank of England Discussion Paper 01/18, July 2018.

To offset the amplifiers from the previous phase, the conceptual model proposes possible systemic mitigants which collectively could represent a macroprudential (or broader) toolkit for systemic cyber risk (see Figure 3). Many of these mitigants are nascent in their development or implementation, and therefore are fertile ground for future study by the ESCG.

3.1.5 Using the conceptual model

In an annex to the above-mentioned Occasional Paper, guidance is provided on how to apply the conceptual model to both hypothetical and historical real-life scenarios. A scenario template has been developed to accompany the conceptual model, which the ESCG has used to compare scenarios (see Section 3.2) and validate the conceptual model. For hypothetical scenarios, the intent was to describe cyber incidents that could possibly lead to systemic events, for example because of the severity of the initial shock or the presence of powerful amplifiers. The analysis does not quantify how long it would take for such scenarios to play out; rather, it looks at which circumstances would need to have occurred for an event to become more systemic. For historical scenarios, past events were assessed to understand the missing factors that would otherwise have resulted in a systemic event. The ESCG developed a “reverse scenario” to back-test the conceptual model, working backwards from the systemic disruption of a specific economic function. Observations and conclusions drawn from use of the conceptual model are described in Section 3.3.

3.2 Scenario analysis

3.2.1 WannaCry

In May 2017, in a matter of a few days, the WannaCry ransomware infected approximately 230,000 computers in more than 150 countries until a “kill switch” was discovered. The



incident is reported to have started on 12 May 2017 in Asia and quickly spread to reach a global scale. A security researcher discovered a kill switch hardcoded into the malware, which helped stop the incident after a few days.

- **Context:** The incident targeted Windows-based computer platforms exploiting a previously known vulnerability for which Microsoft had already issued patches. Companies that had either not applied the patches or were running end-of-life systems were affected. The malware encrypted compromised systems' Master Table File and demanded a ransom of USD 300.
- **Shock:** The encryption of data led to the loss of data and the incapacitation of ICT systems. The UK's National Health Service for instance lost access to some computers, MRI scanners and other ICT infrastructure. Car manufacturers halted production in an attempt to stop the spread of the ransomware.
- **Amplification:** The malware was able to spread automatically in a network. Europol estimates that the cyber incident affected around 230,000 computers in 150 countries, and was as such unprecedented in its scale. Losses were estimated to range between several hundred million to four billion US dollars, which in the event was not sufficient to give rise to general confidence concerns.
- **Systemic event:** In the affected sectors, the incident did not lead to a systemic event due to the quick discovery of the kill switch, as well as the patching of non-infected vulnerable computers. In this instance, the financial sector was not affected, so financial stability was not at risk.

The early discovery of the kill switch significantly helped contain the incident, narrowing down its impact on the global economy. Since 2017, several cybersecurity firms have released software to decrypt files that have been encrypted by the WannaCry malware, helping in the recovery of lost data, thus further reducing the ultimate economic impact.

3.2.2 NotPetya

In June 2017, a series of malicious cyber incidents infected computers of Ukrainian⁶⁷ banks, ministries and companies, which spread to other international organisations with offices in Ukraine, including several major global organisations in the shipping and transport industries. The NotPetya malware was disguised as ransomware, but its intention was to inflict maximum damage by encrypting data and disrupting ICT systems. In contrast to the Petya ransomware, on which it was based, NotPetya not only encoded the Master Boot Record of computers, but encrypted, rewrote or wiped all files on compromised machines in a manner that was not possible to undo by decryption. The ransomware caused widespread damage in Ukraine, including in its financial sector, and affected selected international organisations (outside the financial sector).

⁶⁷ Although Ukraine was the country most affected by NotPetya, this malware also spread to other countries.



- **Context:** The incident targeted Windows-based platforms and combined a sophisticated use of several known vulnerabilities in these platforms and in the M.E.doc software, used by approximately 400,000 users across Ukraine. A backdoor was hidden in installation/update packages of the M.E.doc software. This backdoor was used by the threat actor(s) to compromise the machines running the software. The sophisticated threat actor(s) with high capabilities was likely seeking to disrupt multiple sectors and infrastructures in Ukraine.
- **Shock:** The encryption of data led to the permanent loss of its availability and integrity. This had immediate operational impacts on the affected companies as well as business impacts as several banks, the central bank and major stock markets in Ukraine were disrupted. Elsewhere, damage occurred in selected organisations, albeit outside the financial sector. For example, Maersk, a global shipping company with a 15-20% market share, suffered widespread disruption to its operations.
- **Amplification:** The malware was able to spread through trusted networks at an incredibly high speed, e.g. incapacitating the network of a large Ukrainian bank within less than one minute. In addition, companies with offices and compromised machines in Ukraine, such as Maersk, TNT and Merck, were therefore quickly affected at other locations across the globe.
- **Systemic event:** Official communications and media reports diverge to some extent regarding the assessment of the impact in Ukraine. However, at a global level, there was no impact on major financial institutions or markets.

Only a small number of elements prevented NotPetya from growing into a systemic crisis.

Maersk was seemingly able to recover its data thanks to a single server that was not online by accident and therefore avoided infection. The complete and permanent loss of all data by Maersk could arguably have had systemic repercussions for the global economy. Similarly, had banks and financial institutions in a global financial centre been targeted and incapacitated by the incident, the repercussions would also have been considerably larger.

3.2.3 Cosmos Bank

Cybercriminals launched a sophisticated and highly coordinated attack on Cosmos Bank in India, withdrawing USD 11 million in 14,000 coordinated transactions across 28 countries within two hours. The cybercriminals managed to introduce malware creating a “proxy switching system” that was responding to ATM withdrawal requests, instead of the regular switching system which is part of the core banking system, allowing fraudulent transactions to take place.

- **Context:** Cybercriminals were able to introduce malicious software and send fake authorisations to the ATMs and thus approve a large number of fraudulent transactions at ATMs. The cybercriminals also sent USD 2 million of fraudulent payments in electronic funds transfers and wiped all traces of the incident.
- **Shock:** The shock was limited to an operational impact through the introduction of the malware (creating the proxy switching system), allowing fraudulent ATM withdrawals, resulting in a financial loss totalling USD 13.5 million.



- **Amplification:** While the wiping of logs and traces may have caused some damage to databases of Cosmos Bank, there was no amplification outside of Cosmos Bank.
- **Systemic event:** The losses and operational impact were not sufficiently large to generate any significant contagion that could be of concern for financial stability. Thus, the event did not trigger a systemic crisis.

The incident illustrates the high level of coordination and sophistication of cyber threat actors. It is remarkable that the threat actors coordinated across nearly 30 countries to withdraw funds totalling USD 11 million. The intention was clearly profit seeking, but the level of penetration that the cybercriminals managed to achieve suggests that significantly more damage could have been inflicted on Cosmos Bank, had the threat actors intended to do so.

3.2.4 Hypothetical scenario I: Incapacitation of a large domestic bank's payment system

The ESCG has developed a hypothetical (non-malicious) scenario in which all payment functions of a domestic systemically important bank (D-SIB) are disrupted. The bank is a significant contributor to several retail payment systems. An update accidentally repurposes redundant code in the batch scheduler software and thereby disrupts the payment software and databases of Bank X. As the disruption lasts for a prolonged period of time, financial stress and social unrest begin to materialise. The crisis is compounded by fake news on social media that Bank X has been the target of a sophisticated cyber incident.

- **Context:** The incident is rooted in Bank X's batch software, which controls its payment processing system. The batch software is purchased from and maintained by a third-party supplier. Ahead of the regular nightly run of the scheduled batch of payment orders, Bank X's staff attempts to update a key piece of software. The update includes a maintenance release provided by the third-party supplier. After the upgrade is applied, technicians start to observe batch terminal failures. Upon subsequent investigation, it becomes apparent that the upgrade has corrupted all payment data in the batch jobs. Technicians attempt to enter the batches manually and reload jobs into the queues. However, they fail to reach the key cut-off time for having account balances up to date for the next day. This causes additional recovery problems and further backlogs, creating a cascade effect. At this stage, technicians do not know whether the incident is the result of a malicious incident or not.
- **Shock:** The batch processing system does not run correctly for a while, resulting in millions of transactions not being processed. The incident leads to a prolonged unavailability of account balances at Bank X. Given the complexity of the reconciliation process, there are concerns about data integrity risk.

Business impacts: Bank X is facing a severe operational business impact, and is forced to temporarily shut down all of its retail operations, with an equally severe reputational business impact. While the short-term financial impact is limited, the long-term financial (and legal) impact beyond restoration is expected to be severe (e.g. fines, customer redress, loss of market share).



Technical impacts: The incident leads to prolonged unavailability of account balances. Given the complexity of the reconciliation process, there are concerns about data integrity risk.

- **Amplification:** *Operational to operational:* The unavailability of account balances has a cascading effect and disrupts a wider range of retail services provided by Bank X, as these services rely on the availability of account balance information. Debit cards, credit cards, online and mobile banking applications and cash points are unavailable for a while. The incident has also affected customers of other brands within Bank X's financial group, as all group entities share the same IT environment. The inability of Bank X to reconcile accounts starts to affect its counterparties, as payments from or to customers of Bank X cannot be settled.

Operational to confidence: In addition to not having access to their retail accounts, customers start to worry about the integrity of their balances with the passage of time, leading to a further deterioration of their confidence in Bank X. Customers of Bank X also start to worry about losing their savings, as it is not possible to obtain balance information.

Operational to financial: Bank X is unable to open new accounts and attract funding. Increasing volumes of payments are blocked or delayed. Small and medium-sized enterprises are facing revenue losses due to their inability to use their accounts.

Confidence to financial: Bank X's shares plummet in response to the news of the incident, leading to losses for investors. Bank X is facing increased risk premia in wholesale funding markets due to the uncertainty surrounding the bank's financial situation. Other domestic banks are also facing higher risk premia, as foreign investors have insufficient knowledge about the market to differentiate between Bank X and other banks.

Confidence to confidence: Fake news on social media claiming that Bank X has been the target of a sophisticated cyber incident has fuelled speculation. People have not – or do not know whether they have – received their wages, pensions and/or social benefits and consumers demand access to their accounts. Small and medium-sized enterprises with account balances at Bank X are facing revenue losses as they are unable to send or receive payments, disrupting their economic activities. Customers of other banks are getting anxious that their bank could experience similar failures and begin withdrawing funds from their deposits. Social unrest has started to spread, as a growing volume of payments are blocked or delayed. During all of this, Bank X and the authorities have attempted to calm the public by stating that the situation is under control. However, the inability to provide more details on the nature of the cyber incident and a clear timeline for when the bank will be operational again means that it is not possible to expose the fake news on social media, further fuelling public concerns. This, combined with the inability of Bank X and the authorities to resolve the situation quickly, leads to a broader loss of public confidence in the financial system.

- **Systemic event:** In this hypothetical scenario, all retail operations of Bank X have been shut down. Both online banking and physical cash points of Bank X are unavailable. Customers have been unable to access their current account balances, make payments and receive payments for a prolonged period. Despite ongoing efforts to respond and recover, Bank X has been unable to reconcile account balances, and uncertainty regarding the scale and duration



of the incident increases. A while after the original incident, the software provider finds out that the upgrade had accidentally repurposed redundant code in the batch scheduler software, which reformatted data in the batch jobs such that the software was not capable of reading the data properly.

The prolonged disruption of a significant part of a country's payment system combined with uncertainty and fake news spreading through social media could trigger large-scale financial instability. In this hypothetical scenario, it is possible to imagine a number of further aggravating circumstances and failing business continuity plans. A key point to consider is that a loss of confidence in one financial institution may quickly spread to become a general loss of confidence in similar institutions or the financial sector at large. The hypothetical example illustrates how a perceived cyber incident that initially leads to the unavailability of deposits and account information could spiral into liquidity problems for other banks that were initially not affected by the cyber incident but are suffering from the loss of confidence in the financial sector. It should be noted that the incident at Bank X was not malicious. Nonetheless, the presence of large-scale and long-lasting operational disruption, together with initial uncertainty about the nature of the incident and subsequent social media speculation about possible cyber activity, combine to give this operational event features of cyber stress, in turn contributing to greater systemic risk.

3.2.5 Hypothetical scenario II: Malicious destruction of account balance data

The ESCG has developed a second scenario in which account balances, and other data related to value, have been seemingly permanently destroyed. Threat actors are launching an attack on the account balance data and payment software of a large bank, leading to the loss of availability and integrity of account balances with severe impacts on both wholesale and retail clients.

- **Context:** Threat actors have accessed the IT systems of Bank Y combining the use of malicious software exploiting vulnerabilities and the infiltration of technical staff in outsourcing contractors of the IT systems management supply chain. Without being detected for months, they have monitored the financial institution's operations and gained access to administrator rights for various critical systems. During that time, the threat actors have also been able to compromise the data backup and restoration processes of these critical systems. At a sensitive date and after having retrieved a considerable amount of confidential information, the threat actors initiate a large-scale incident impacting the integrity of data within the critical systems under their control: a massive set of unauthorised payments are performed, data of Bank Y's payment-related processes are wiped, software related to the payment services is altered, and the account balance data of a large number of accounts is also wiped.
- **Shock:** At first, only Bank Y is impacted. Bank Y suspends the operations of its payment systems, because they are not reliable. Soon after, second-order impacts (e.g. on its customers) are noticed. Manual workarounds, prioritising certain types of payments, prove manageable in the short term, but there are concerns that this could lead to a significant backlog. The practicality and effectiveness of such workarounds also depend on the



resumption of operations and the availability of data at a later stage. A further concern is that available information is not reliable. The event is communicated to the national competent authority (NCA) under the NIS framework and under supervision and oversight frameworks. Early on, it appears that the crisis involves the main branch of Bank Y, as well as its subsidiaries in other countries, as the IT systems of the banking group are centralised. The NCAs of the countries concerned are therefore informed. Bank Y also provides information about the incident to the constituency of the Financial CERT (in an anonymised way).

- **Amplification:** At this stage, whilst the recovery time is unknown, Bank Y is working under the assumption that it will be able to resume services and that essential data will be restored before the manual workarounds and other contingencies cease to be viable. As time goes by, the institution's critical activities exceed their maximum tolerable downtimes because of IT service unavailability.

Operational to operational: Bank Y's crisis management team decides to activate business continuity plans, in the belief that (most of) the data will be restorable from backups and operations will be performed via alternative redundant platforms. However, as the malicious actors were able to alter technical recovery procedures, it becomes apparent that business continuity plans have become ineffective. Because of the interconnectedness of account balance data, payment systems and treasury procedures, the operational disruption of Bank Y has immediate consequences for treasury services and procedures, which are time-critical; by the end of the first day, Bank Y's receipts and payments are in a pending status.

Operational to financial: Many institutional customers (financial and non-financial institutions alike) did not receive payments or credit that they were expecting. Moreover, customers are unable to use funds from their deposits, thus increasing the severity of the impact. Bank Y's management reaches the view that there is a possibility that impacted data are lost permanently, or that recovery would at least take a considerable amount of time, possibly exceeding several weeks. External experts and providers are asked for support and attempt to set up alternative platforms. Regarding Bank Y's own liquidity position, marginal lending facilities, emergency bilateral agreements and/or – depending on the framework – emergency liquidity assistance from Bank Y's central bank could be set up. This presumes however that the disruption is perceived as temporary and the bank viewed as solvent. Note that, in this respect, a more severe scenario where threat actors had further incapacitated the collateral framework of Bank Y would make posting collateral to receive emergency liquidity from the central bank more difficult. The financial situation of Bank Y deteriorates because it cannot perform payment, clearing and settlement services. Indeed, the further incapacitation of Bank Y's collateral framework would also render the bank unable to meet margin calls (e.g. from central counterparties (CCPs)) and likely trigger default management procedures, and could potentially trigger the intervention of resolution authorities.

Operational to confidence: Bank Y's customers become concerned. There is a spike in attempted cash withdrawals from ATMs and branches, of which the majority fail due to the disruption of the account balance data and payment systems. The bank suffers a surge in call centre calls from customers seeking to understand the impact of the problem and wishing to establish whether their money is safe.



Confidence to confidence: In a more severe scenario, the threat actors could further disrupt public confidence by claiming responsibility for the incident at Bank Y, stating that they are able to repeat such action at other banks. Social media are used to spread rumours, which amplify the erosion of confidence in the financial system at large.

- **Systemic event:** Eventually Bank Y becomes aware that it is not possible to recover its data, at least in the short term. It is likely that data could be recovered from a specific Recovery Point Objective (RPO), but the time to resume operations is not negligible. The bank is therefore obliged to build new systems from scratch, trying to recover data through semi-manual procedures, all of which will take more time. The bank informs the authorities, the market and its customers. The impact on the operations of other intermediaries, market operators and customers has now reached a systemic level: both Bank Y and several of its counterparties report liquidity problems, whilst the country's payment, clearing and settlement systems are also experiencing disruption.

Financial firms look to the authorities for direction, since they cannot tackle the issue alone. The authorities look at countermeasures to support and coordinate recovery from this scenario and are exploring whether market participants could work together to identify offsetting positions with Bank Y across the market and whether there is scope to net these off. The loss of confidence plays a major role: customers seek to move their funds to other banks, but this would depend on the availability and integrity of balance information, which is not the case, causing the situation to escalate further.

A key concern for authorities and the public at large is whether account data are (perceived to be) permanently lost, or whether they can be recovered. Bank Y's communication strategy for the duration of the event is therefore critical. And it will become increasingly difficult to maintain, especially as it becomes less certain that all data can be recovered. The intention of the threat actor also plays a key role. If the objective pursued is the disruption of the financial system, it is likely that business continuity plans would have been tampered with and that social media campaigns would be actively used to stir unrest and panic.

3.2.6 Hypothetical scenario III: Scrambling of price and position data

The third hypothetical scenario developed by the ESCG explores the manipulation of price feeds and position information, which leads to distressed liquidations and severe market turmoil. Malicious actors have managed to manipulate the price feeds of several commodities and futures markets, as well as the trade and position information that market participants are receiving from the market's CCP. As uncertainty spreads regarding the reliability of prices and positions, traders are pulling out of the market causing liquidity to drop, prices to drop sharply and automatic stop losses to be triggered. The ensuing market panic takes on a self-reinforcing and self-sustaining dynamic which causes severe losses for multiple market participants across several market segments.

- **Context:** Market data providers and a CCP are simultaneously targeted in the incident. The threat actors have managed to insert malicious code into the ICT infrastructure used for the



processing and outputting of price, trade and position data. The malicious software has the capability to selectively modify the data that are being received or sent.

- **Shock:** The malicious code, which manipulates incoming and outgoing data, is activated at a commodity and futures CCP, as well as at several related market data providers. This results in random errors for entered trades, trade rejections, errors in the reporting of current positions and conflicting market prices observed by market participants.
- **Amplification:** *Operational to operational:* The immediate impacts are a number of trade novation failures and incorrect risk reports that have received erroneous market prices and positions as inputs. Consequently, final settlement of the respective trades does not take place.

Operational to confidence: Affected market participants begin doubting the accuracy of reported prices and positions. As the malicious code does not affect all positions, prices and trades, it may make the identification of the incident more challenging. Although not immediately diagnosed as a market-wide problem, there is widespread uncertainty and a growing sense of unease among market participants.

Confidence to operational: While some market participants are unwilling to enter new trades and adopt a “wait and see” approach, others start trying to bypass regular trading channels and attempt to trade bilaterally, disintermediating the CCP, for assets for which clearing is not mandatory (or the obligation is temporarily suspended). As they continue to worry about the reliability and accuracy of prices, some traders begin exiting positions.

Confidence to confidence: As more and more market participants become unwilling to trade, market liquidity falls, adding further doubts regarding the state of the market. A self-reinforcing loop is beginning to emerge.

Confidence to financial: Due to the drop in liquidity and traders seeking to exit positions, volatility increases and prices continue to fall. The risk management framework of the CCP is severely incapacitated due to inconsistent price information. As a precautionary measure, the CCP may increase initial margin levels.

Financial to financial: Automatic stop losses are triggered. These are generating a new wave of sell orders across multiple market segments. This further increases price drops and volatility spikes and feeds negatively into the confidence channel. As prices fall further, the CCP will issue margin calls to members, potentially triggering the default of some firms that are unable to meet the margin calls within the required timeline.

- **Systemic event:** In the absence of circuit breakers and a strong intervention by the authorities, large numbers of investors (or market-makers) seek to “run to the exit”, further depressing prices. In the given scenario, the problem is not immediately identified as an operational issue or cyber incident. Hence, the authorities misinterpret the market turmoil as changes in expectations and a repricing of risk, and are hesitant to intervene. However, as the disruption continues and a self-fulfilling loop of distressed liquidations has been triggered, losses accumulate. The scenario thus moves from a cyber incident to a market liquidity crisis, with multiple “liquidity spirals”. The longer the disruption, the greater the losses triggered by



stop losses. In a severe variant of the scenario, this leads to the defaults of, for example, commodity firms, with further second-round effects affecting a range of markets and asset classes. Depending on the severity of the price drops and the default management procedures of the CCP, in an extreme case of the scenario, it is conceivable that the CCP would incur losses exceeding its default fund, triggering the default of the CCP. This would exacerbate the stress suffered by the market significantly.

While tampering with price and position feeds is unlikely to create a stress event akin to a financial crisis, in the given scenario, severe market disruption including the default of certain trading firms, and potentially the affected CCP, materialises. Unless the ensuing market turmoil has extremely severe repercussions (as noted above), the losses that materialise are unlikely to be sufficiently large to trigger a large number of defaults so as to endanger financial stability. Nevertheless, the market turmoil may well be sufficient to incapacitate markets for several days. In this scenario, the threat actor could have been motivated by either financial profit seeking (e.g. by placing appropriate short orders) or the desire to cause damage to the real economy by disrupting closely linked market segments (e.g. commodity markets and futures markets).

3.3 Grouping and prioritisation of common individual vulnerabilities

In this section, the ESCG offers a view on the grouping and ranking of the common individual vulnerabilities. Section 2.4 presented the list of the CIVs which the ESRB identified as having a direct causal link to cyber incidents. However, the vulnerabilities were not prioritised or grouped at that stage, which is the objective of this section. As vulnerabilities may be associated with a range of cyber incidents, it is difficult to establish a robust ranking (from the most to the least important vulnerability). Instead, the ESCG proposes two broad categories: (i) vulnerabilities that may have a direct and amplifying effect; and (ii) broader “enablers” (i.e. vulnerabilities with no direct causal link to the cyber incident). These are referred to as “impact categories”.⁶⁸

Table 4 provides a tentative ranking of the CIVs by considering: (i) their prevalence in ESRB member jurisdictions; (ii) supervisory and oversight priorities (as explained in Section 2.4.); and (iii) the impact categories mentioned in the previous paragraph. The ESRB judges the top three CIVs to be:

- process-based CIVs: these are caused by flaws/weaknesses in controls, testing processes and measures and/or gaps in internal processes, rendering an organisation more vulnerable;
- CIVs capable of direct causation: these may have a direct and amplifying effect; and
- highly prevalent CIVs.

The ESRB notes that this is a conceptual exercise and there is no evidential basis that any given CIV is more likely to lead to a systemic event than another. Hence, the proposed ranking should not

⁶⁸ Further details can be found in “The making of a cyber crash”, *ESRB Occasional Paper Series*, Forthcoming.



be taken as exhaustive or overly authoritative. Furthermore, the ESRB is of the view that cyber resilience requires a holistic approach, which is inconsistent with a strong prioritisation on the basis of a conceptual model. Doing so could encourage authorities to focus on a subset of issues and could promote a false sense of security. There may be a correlation between CIVs and a higher frequency of cyber incidents at individual institutions, but it is not possible to infer a systemic link from this correlation alone.

Table 4

Common individual vulnerabilities likely to have contributed to a cyber incident

Rank	Common individual vulnerability (CIV)	Causation	Prevalence
1	Insufficient industry oversight of third party suppliers and supply-chain	Direct	1
2	Inadequate cyber hygiene	Direct	2
3	Ineffective testing of people, processes and technology	Direct	5
4	Insufficient cyber strategic planning and board level influence on cyber resilience	Indirect	3
5	Lack of investment in cyber threat intelligence	Indirect	4
6	Presence of end of life systems	Direct	6
7	Technology centric focus underestimating responsibility of people and processes	Indirect	7
8	Organisational culture change needed for secure cybersecurity behaviours	Indirect	8
9	Cyber undermines existing operational resilience arrangements	Direct	9
10	High risk internet use requires better controls	Direct	12
11	Firm scale and resources impact effective cyber risk management	Indirect	10
12	Insufficient credible third line of defence challenge in firms	Indirect	11
13	Cyber maturity targets not defined	Indirect	13

Source: ESRB (ESCG).

3.4 Main findings of the vulnerability analysis

This section summarises the main findings of the ESRB's analysis of the vulnerabilities in the context of the systemic cyber risk framework.

Mitigating vulnerabilities is important in order to reduce the likelihood of cyber incidents, but is unlikely to eliminate them altogether. The rigorous testing of IT change management processes and batch updates is a crucial element that helps reduce the risk of unintended failures. Additionally, increased cyber hygiene or oversight of third-party suppliers and the supply chain could reduce the scale and impact of an incident where previously known vulnerabilities that were not or could not be patched were exploited.⁶⁹ However, given that firms cannot eliminate the

⁶⁹ As per the examples of WannaCry and NotPetya.



likelihood of a cyber incident altogether, a key issue for financial service providers as well as all relevant actors in the sector is to be prepared for cyber incidents and establish sound response and recovery processes.

A general loss of confidence in the financial system as well as (an anticipation of) large financial losses are two key factors that determine whether or not a cyber incident becomes systemic. The scenario analysis in Section 3.3 illustrates the critical roles that confidence, as well as the magnitude and distribution of financial losses, play in assessing whether or not a cyber incident may escalate into a systemic (financial) crisis. An operational incapacitation of a large part of the financial infrastructure need not trigger a systemic crisis. Indeed, the likelihood and/or impact of a system-wide outage could be mitigated through temporary solutions and workarounds. However, such measures critically rely on trust among counterparties. In this respect, there is a subtle but crucial difference between two financial institutions being unable to lend to each other and their being unwilling to lend to each other. An anticipation of large financial losses may reduce this trust between counterparties and thereby frustrate ad hoc workarounds. The anticipation of large financial losses and/or a critical mass of rumours in social media could also prove sufficient to trigger a classic bank run by customers.

An inadvertent (seemingly permanent) distortion of data integrity could have systemic consequences. An accidental failure that compromises the integrity or availability of data related to value (account balances, securities holdings, etc.), which the institution in question would not be able to confirm as fixable in a short time, could be a sufficiently severe shock to confidence, which in turn could spark market turmoil and trigger a spiral of events that could escalate into financial stability concerns.

The threat actors' intention to disrupt or destroy plays a key role and increases the likelihood of a systemic outcome. A malicious cyber incident involving a threat actor motivated by profit seeking alone is less likely to generate sufficiently large losses to trigger a systemic crisis. Such big losses and the disruption of confidence are more likely to occur when the threat actors' intention is to destroy or disrupt parts of the financial system, rather than steal funds. Widespread and irrecoverable encryption, deletion or modification of critical data are examples of how a systemic crisis could be triggered. By contrast, it is difficult to conceive that a threat actor would be able to make fraudulent transfers of a sufficient magnitude to be able to trigger financial stability concerns. For instance, if – in the aftermath of a successful malicious cyber incident – the customers of a bank were to find all account balances to be zero or unavailable for a prolonged period of time, and the institution were to be unable to resolve the situation within a reasonable time frame, it is conceivable that panic could start to spread. As a complicating factor, in such an instance fake news and disinformation may spread via social media, potentially as part of the incident, further destabilising the markets and society.

The time at which a cyber incident occurs as well as its duration are also important factors in determining the impact on confidence. For instance, the incapacitation of a payment system in the midst of severe market turmoil would have far larger ramifications than under normal market conditions and circumstances. Similarly, the amplification through the confidence channel is sensitive to the duration of the event: the longer a cyber incident is ongoing, the higher the likelihood that the confidence channel would be materially triggered (e.g. a higher likelihood of rumours and fake news spreading, and credible communication becoming increasingly difficult).



The maintenance of confidence in the system and the management of (crystallised) systemic cyber risk require rapid and sophisticated communication and action plans to be implemented by the relevant financial and non-financial authorities. The speed at which cyber incidents crystallise implies that there may be insufficient time during the unfolding of an incident to create such plans at the time of need.

Overall, cyber risk has evolved from being an operational risk with a limited potential impact on financial stability to a systemic risk with the potential for severe impacts on financial stability and the real economy. The analysis presented in the previous sections points towards the fact that, with an unfortunate alignment of factors, the materialisation of cyber risk could have sufficiently severe consequences so as to spark large-scale financial instability and potentially a systemic crisis. The scenario analysis further suggests that both accidental cyber incidents as well as those arising from malicious activity can have a material impact on financial stability.



4 Conclusions

4.1 Summary

In the absence of historical precedents, the ESRB has examined whether, and if so how, a cyber incident could cause a systemic crisis. To this end, the ESRB's European Systemic Cyber Group developed a conceptual framework and applied it to a range of historical and hypothetical scenarios. The aim of the analysis was to explore how, in certain circumstances, a cyber incident could lead to a systemic crisis, defined as "disruption in the financial system with the potential to have serious negative consequences for the internal market and the real economy". This report explored how a cyber incident could create widespread disruption in the financial system. The main discussion in Section 3 started by focusing on a number of cyber incidents, each of which had the potential to harm the real economy, because:

- the normal functioning of critical economic functions had been severely disrupted ("operational disruption channel");
- the disruption spread to other critical economic functions that were not targeted by the cyber threat actors ("operational contagion channel"); and
- the disruption undermined public and market confidence, in turn triggering (known) financial contagion channels, and resulting in either a liquidity crisis (as defined in the financial stability literature) or the insolvency of major financial institutions (or both).

Section 3 also argued that whether or not a cyber incident would cause such significant harm depended on a number of factors, including:

- the context;
- the nature of the shock;
- the presence of several amplifiers; and
- the presence of effective risk mitigants.

The analytical framework suggests that a truly systemic event would require a severe shock, an alignment of amplifiers and a lack of effective systemic mitigants. As argued throughout the report, the financial system displays a number of vulnerabilities, which together create a context in which a systemic cyber crisis could unfold. In all of the hypothetical scenarios presented in Section 3, the greatest damage to the financial system occurred when multiple amplifiers were activated and what was initially an operational crisis triggered a sufficiently severe loss of confidence in financial institutions and markets. Furthermore, the hypothetical scenarios indicated that financial market participants on their own would not be able to resolve the crisis, but instead required support from financial and non-financial authorities.



A system-wide operational outage need not lead to a systemic crisis, but the scenario work provides examples of where a cyber incident could trigger such an outcome (in these instances through a liquidity or “traditional” financial crisis). All three hypothetical scenarios were characterised by severe liquidity pressures, reflecting participants’ inability to access normal payment channels, either because critical systems were disabled or critical data were corrupted or deleted. However, the key tipping point in each of the scenarios examined occurred at the point at which the confidence in the financial system was so severely weakened that important financial institutions would cease all lending activity. In other words, at the heart of all three hypothetical scenarios is the critical transition from a state where the important financial institutions *are not able* to lend to each other to a state where they *are no longer willing* to lend to each other. The analysis presented illustrated how a cyber incident could, under certain circumstances, rapidly escalate from an operational outage to a liquidity crisis. In turn – and in common with historical financial crises – this liquidity crisis could, in certain circumstances, lead to a systemic crisis. This could happen, for example, if the size of anticipated losses were to be very large. Thus, the later stages of a systemic cyber crisis as demonstrated through the scenarios are similar to those seen in more “traditional” financial crises: large (expected) financial losses and a significant weakening of the trust in the financial system.

The analysis conducted by the ESRB shows that it is indeed conceivable that a cyber incident could evolve into a systemic cyber crisis that threatens financial stability. The historical and hypothetical scenario analyses reveal that the exploitation of vulnerabilities together with an ill-fated alignment of systemic amplifiers make a systemic cyber crisis a conceivable event.

Additional efforts are required to reduce the potential impact of such a crisis and the likelihood of it happening. As indicated in Section 2, both public authorities as well as private entities are undertaking a significant number of initiatives to reduce cyber-related risks. While the characteristics of cyber risk make it extremely difficult (or costly) to fully eliminate it, there are a number of policy areas that deserve more exploration to identify and mitigate systemic cyber vulnerabilities, thus further reducing systemic cyber risk. Without taking a stance, the next section explores some of these options. In some instances macroprudential tools may be appropriate, while in others (traditional) central bank intervention may be required. Microprudential supervision, an improved level of cyber hygiene and a collective industry response are additional key building blocks.

4.2 Policy areas and potential options

The scale and rapidity at which cyber incidents can unfold require a response by authorities at an unprecedented speed, which in turn requires a high level of planning and preparation.

To date, the financial sector has not experienced any cyber incidents that have threatened financial stability. However, as argued in the previous section, an intentional incident with the goal of destabilising the financial system could, in certain circumstances, trigger a systemic crisis. Moreover, the circumstances of such a crisis may be unprecedented, suggesting that financial authorities need to consider the range of policy options that may be required, both on an ex ante basis to reduce the probability and impact of a severe cyber incident, and on an ex post basis to intervene in a timely and focused manner, should this be required. In particular, the speed and

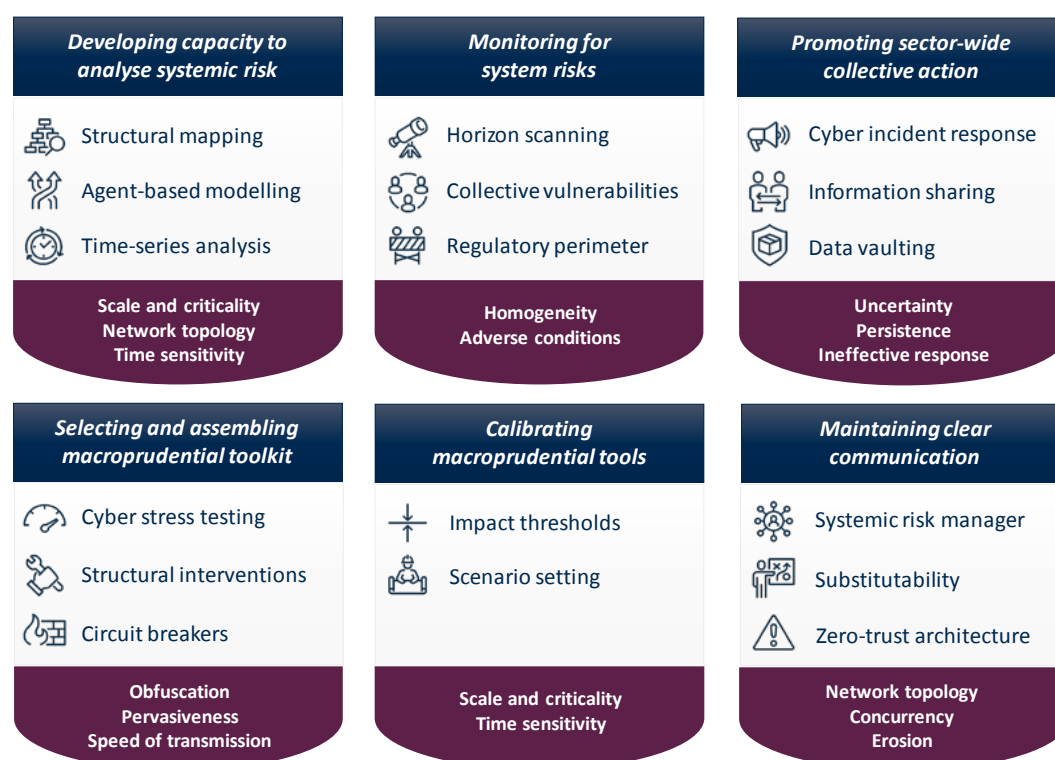


scale of an unfolding cyber incident require macroprudential authorities and central banks to reflect on and operationalise their responses, coordination and communication plans in the event of different types of cyber incidents *prior* to their occurrence. While bearing in mind the costs of such endeavours, existing initiatives such as the G7 cyber exercises or comparable domestic exercises may be leveraged on to test and possibly improve current coordination and communication policies.

The threats posed by systemic cyber risk require further work by macroprudential authorities.

Figure 3 provides a non-exhaustive overview, attempting to group together some of the systemic mitigants – linked to the system's shock amplifiers – that could form part of a macroprudential toolkit for systemic cyber risk management. A key similarity among all options is their pre-planned character. The features of cyber risk make it unlikely that ad hoc solutions would suffice to address the risk. Some of the options are explored in further detail in the following paragraphs. It should also be noted that macroprudential authorities are likely to work closely with microprudential authorities (which may have incorporated cyber resilience into their supervisory frameworks) and with the financial industry, whose collective action programmes can advance work addressing vulnerabilities and play a key role in improving industry readiness to deal with an actual crisis.

Figure 3
Examples of systemic mitigants that could constitute a macroprudential toolkit for systemic cyber risk and the amplifiers that they could offset



Source: ESRB (ESCG).



Vulnerabilities are persistent and financial institutions may not always have sufficient incentives or means to mitigate systemic cyber risk.

Macroprudential authorities want to highlight the need to address these vulnerabilities as they create the context for a cyber incident to develop into a serious crisis, with the potential to threaten financial stability. A number of the common identified vulnerabilities, such as “insufficient industry oversight of third-party suppliers and the supply chain” or “inadequate cyber hygiene”, have not recently emerged. Rather, these are persistent vulnerabilities that require continuous attention as technology evolves and the threat landscape changes. Supervisory guidelines cover a large part of these cyber-related risks and institutions moreover have a private incentive to minimise cyber-related reputational risks that could arise, for example, from idiosyncratic incidents such as the theft of client funds or data. The overall level of awareness of financial institutions of the need to improve protection, as well as the preparedness for crisis situations, have increased over the last years. However, and not unlike other types of systemic risk (climate change-related risk, geopolitical risk, etc.), investing in further improving resilience against this tail risk also requires collective (rather than individual) action by firms.

Cyber risk poses new challenges for macroprudential authorities. Whereas mitigating the immediate (technical) impacts of a cyber incident on individual institutions tends to fall more into the realm of microprudential or supervisory authorities, macroprudential authorities and central banks may well need to deal with the broader consequences of a cyber incident. To the extent that the cyber incident creates liquidity pressures, existing liquidity regulation may provide a sufficient shock absorber. But the disruption caused by a cyber incident may affect the actual use of existing liquidity buffers. As a result, and given the centrality of liquidity in systemic risk scenarios, there is a specific role for central banks to reflect on the challenges to their traditional tools and emergency plans. For example:

- To what extent can microprudential capital requirements for operational risk absorb the potential financial impact of a systemic cyber incident?
- Should, and if so, how could central bank emergency liquidity assistance frameworks be operationalised in the event of a systemic cyber crisis?
- Is there a role for circuit breakers?
- What are the options for data recovery, in particular in those instances that require the transfer of the functions of a disabled organisation?

Finally, close cooperation as well as a clear division of tasks between technical teams dealing with technical incident management, on the one hand, and central banks dealing with the (financial) consequences of the incident, on the other hand, are critical.

The ESRB intends to explore some of the systemic mitigants in future work. Taking stock of the findings in this report, the ESRB intends to leverage its broad institutional composition and network to evaluate the costs and benefits of different systemic mitigants going forward.



Annex 1: Report on common individual cybersecurity vulnerabilities

Introduction

This annex sets out the common individual cybersecurity vulnerabilities (not threats) identified by ESRB members across the supervised entities. It explains the methods used to identify and assess these vulnerabilities. Based on a microprudential analysis undertaken in the respective jurisdictions, it does not take into account the systemic aspects of the vulnerabilities.

The increased threat of cyber incidents has the potential to disrupt financial services and threaten the stability of the financial system. It is therefore important that coordinated efforts are taken to prevent and mitigate these risks. A common understanding of the vulnerabilities and supervisory approaches is necessary to provide a starting point for moving towards such a coordinated effort.

This annex is based on the answers to a questionnaire completed by the competent authorities of 14 EU Member States in 2018 and lists common individual cybersecurity vulnerabilities. For a discussion of their relevance, please refer to Section 2.4 of the main report. This section follows a bottom-up approach starting from the microprudential perspective, collecting and aggregating common thematic cybersecurity vulnerabilities identified at a national level. In this regard, the annex presents the prevalence and prioritisation of the identified common individual vulnerabilities across the ESRB jurisdictions. Table A.1 provides a brief explanation of each common individual cybersecurity vulnerability.



Table A.1

Brief explanation of each common individual cybersecurity vulnerability

Vulnerability	Explanation
1. Cyber issues undermine existing operational resilience arrangements	Cyber issues have been found to undermine existing resilience arrangements and call for the reassessment of operational resilience approaches as the characteristics are very different. Firms have not taken the broader issue into account and rarely analyse risks across silos. The majority of firms have provisions in place for malicious operational disruption or DDoS incidents affecting their internet-facing systems; however, these mechanisms are rarely tested as part of a larger recovery testing plan.
2. Insufficient cyber strategic planning and board-level influence on cyber resilience	The effectiveness of cyber-resilience measures is undermined by deficiencies in board-level influence, organisational design, the operating model and strategy.
3. Cyber maturity targets not defined	Firms in the sector voice frustration in trying to articulate a credible target state of maturity for their cyber programmes. The firms derive required domains of practice from standards, but there is a lack of clarity about what an appropriate level of cyber sophistication would be. This has a direct impact on the allocation of cyber investment funds and presents a prevalent risk of misallocation and supervisory friction. A root cause is the thematic issue of firms underinvesting in situational awareness; hence, risk and investment decisions are based on insufficient or incorrect information.
4. Insufficient industry oversight of third-party suppliers and the supply chain	Firms in the sector tend to have an inadequate approach to the oversight of their supply chain and third parties, which often provide their information processing or IT systems. As a result of outsourcing, it is highly complex for institutions to have effective oversight over their critical service providers' management of cyber risk. The approach tends to rely on assurance from audits rather than effectiveness testing and continuous partnerships and collaboration with critical suppliers.
5. Insufficiently credible third line of defence challenge in firms	The majority of firms assessed have had deficiencies in responses from internal audit or an outsourced professional services company as the third line of defence. In some cases, internal audit has been out of touch with cyber developments and avoided reviewing the common large-change programmes and instead concentrated on thematic control sampling, which provided limited assurance.
6. Ineffective testing of people, processes and technology	The sector does not conduct adequate cyber effectiveness testing across people, processes and technology. Assurance is largely gained through audits and control sampling, which is not sufficient. Firms rarely make an internal business case for cyber risk management and effectiveness testing of what a firm gets for its investments is rarely conducted. Some firms neither have adequate business continuity planning with scenarios featuring the materialisation of malicious cyber incidents, nor do they have response plans for cyber incidents.
7. Firm scale and resources impact effective cyber risk management	A firm's size and available cyber resources have been found to have an impact on effective cyber resilience. Smaller firms struggle to keep up with change due to limited resources. Larger firms with substantial resources struggle due to challenges in managing change at pace and on a large scale. Medium-sized firms with above average resources seem to be managing better, while there is still room for improvement.



Vulnerability	Explanation
8. Technology-centric focus underestimating responsibility of people and processes	Firms incorrectly view cyber matters as a technology issue and are technology-centric in capability building. This can lead to an imbalance between investment in technology and investment in human capital, with a limited strategic vision regarding skill development, team composition and succession planning. This can erode cyber resilience over time and reduces the return on the technology investment.
9. Lack of investment in cyber threat intelligence	Some firms are underinvesting in their capability to detect cyber incidents in progress and to identify threats which are external and internal to the organisation (situational awareness). The sector's ability to collect, analyse, consume and share threat intelligence tends to be immature, as it tends to be too technical and tactical to be effective in the long term. Firms' ability to detect advanced cyber incidents tends to be immature as firms struggle in collecting and analysing indicators of malicious activity and tend to underinvest in both detection and analysis capability. Additionally, firms' fraud detection systems are not integrated with cyber incident identification tools.
10. Organisational culture change needed for secure cybersecurity behaviours	Some firms are underinvesting in organisational culture change to drive secure cybersecurity behaviours and buy-in. Firms tend to adopt a "technology-first" approach to cyber issues to the detriment of investment in people. There is a clear skill-set gap when it comes to driving behavioural change initiatives, which is related to the theme of deficiencies in leadership capability.
11. High-risk internet use requires better controls	Some firms appear to struggle to maintain an adequate separation between critical IT services and staff members' high-risk internet use, which could provide a route for threat actors to access or interfere with those critical IT services. High-risk internet use on staff PCs includes email and web browsing, which are the two most popular methods for threat actors to gain access to corporate networks.
12. Inadequate cyber hygiene	Cyber hygiene, which involves having practices and processes in place to improve cybersecurity, is not yet consistently followed in some firms. In particular, the secure configuration of IT systems, the management of user credentials in identity management and general network security can together protect the confidentiality, integrity and availability of systems and information. Cyber hygiene issues can also be seen in the lack of, or inadequate, information asset classification and management, which should be carried out in accordance with the confidentiality, integrity and availability criteria in order to protect the assets. Some firms have slow patch management despite recognising that known vulnerabilities need to be rapidly resolved. This leaves the systems vulnerable to exploitation.
13. Presence of end-of-life systems	Many firms exhibit the presence of "end-of-life systems" (i.e. those systems that have been active for longer than they were designed to run), which is indicative of poor cyber resilience. Examples of out-of-date commodity software include the use of Windows XP and Windows Server 2003, which are out of standard support and thus may present a higher risk as there are known vulnerabilities in relation to them.

Identification of cyber vulnerabilities

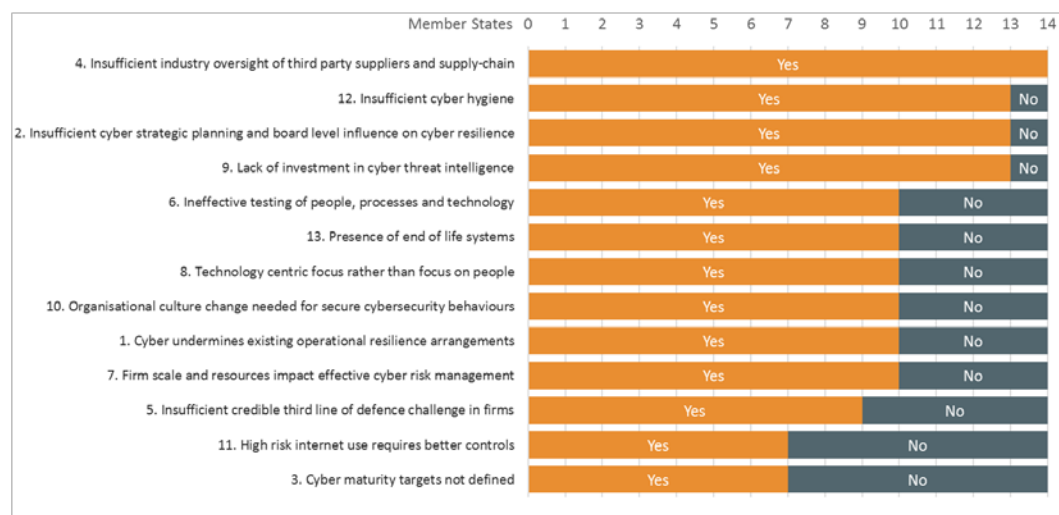
Chart A.1 demonstrates the degree of prevalence of the list (see Table A.1) of cyber vulnerabilities (based on the number of Member States in which the same vulnerabilities were identified). This, however, does not imply the severity of the vulnerabilities or mean that a particular vulnerability has materialised in the jurisdiction concerned; only that it has been noted to exist.



Insufficient industry oversight of third-party suppliers and the supply chain (vulnerability 4) is the most prominent vulnerability common across all 14 ESRB jurisdictions that have responded to the questionnaire.

Chart A.1

Prevalance of each of the common individual vulnerabilities identified in the questionnaire



Source: ESRB (ESCG).

Inadequate cyber hygiene (vulnerability 12), insufficient cyber strategic planning and board-level influence on cyber resilience (vulnerability 2) and the lack of investment in cyber threat intelligence (vulnerability 9) were mentioned by all but one respondent Member States, demonstrating that these vulnerabilities have been recorded in all other jurisdictions.

Overall, all common cyber vulnerabilities have been recorded by at least half (seven out of 14) of the respondents.

Thematic grouping of cyber vulnerabilities

The ESCG organised its thematic findings under 13 headings (see Chart A.2). Four findings were found in almost all of the 14 jurisdictions that contributed to this assessment. These are:⁷⁰

- **Insufficient cyber strategic planning and board-level influence on cyber resilience:** The effectiveness of cyber-resilience measures is undermined by deficiencies in board-level influence, organisational design, the operating model and strategy.
- **Insufficient industry oversight of third-party suppliers and the supply chain:** Firms in the sector tend to have an inadequate approach to oversight of their supply chain and third parties, which often provide their information processing or IT systems.

⁷⁰ Note that this ranking reflects the supervisory prioritisation as described further below in this section of the Annex.



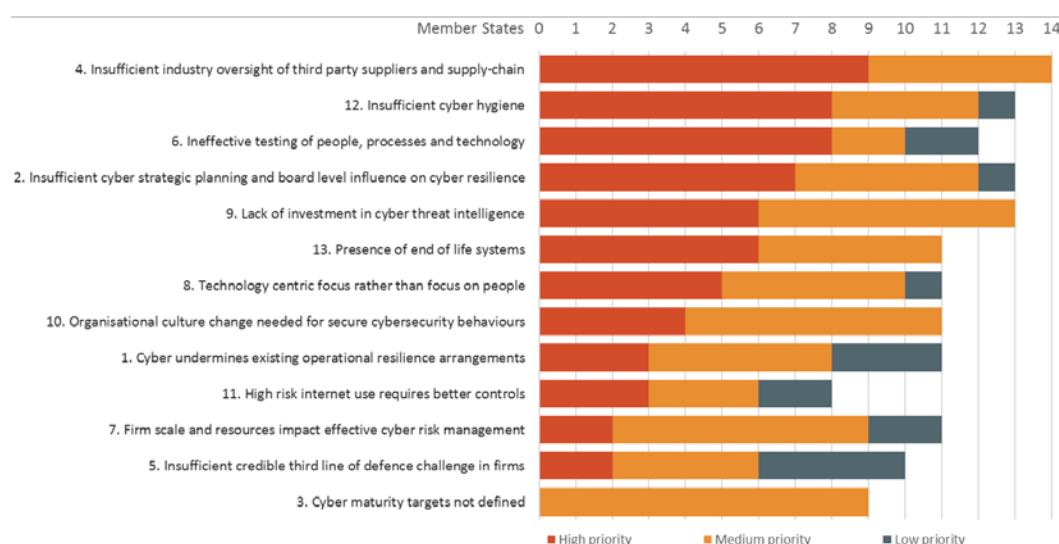
- **Ineffective testing of people, processes and technology:** The sector does not conduct adequate effectiveness testing of the prevention and detection of and the response to cyber incidents across people, processes and technology. Assurance is largely gained through audits and control sampling, which is not sufficient.
- **Inadequate cyber hygiene:**⁷¹ Cyber hygiene, which involves having practices and processes in place to improve cybersecurity, is not yet consistently followed in some firms. Hygiene practices include (but are not limited to) the secure configuration of IT systems, the management of user credentials in identity management and general network security, which can together protect the confidentiality, integrity and availability of systems and information.

Respondents provided views on the prioritisation rating of each vulnerability (assigning high, medium or low priority to each vulnerability). Prioritisation is based on individual jurisdictions' supervisory judgements and is not based on the potential systemic impact of the vulnerabilities. The top three cyber vulnerabilities in terms of priority ranking (with "High priority") are:

- insufficient industry oversight of third-party suppliers and the supply chain (vulnerability 4);
- inadequate cyber hygiene (vulnerability 12); and
- ineffective testing of people, processes and technology (vulnerability 6).

Chart A.2 illustrates the prioritisation of the vulnerabilities provided by ESRB members.

Chart A.2
Supervisory prioritisation rating of each of the common individual vulnerabilities



Source: ESRB (ESCG).

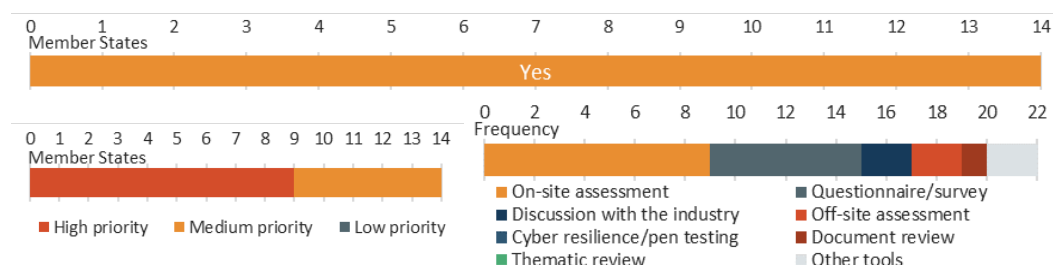
⁷¹ The group discussed how cyber hygiene can involve investing in activities/actions that do not result in a comparative advantage, but – if done poorly – can have devastating consequences.



The main concerns for the top three vulnerabilities as explained by the respondents are summarised below.

Chart A.3

Insufficient industry oversight of third-party suppliers and the supply chain



This vulnerability was viewed as having the highest priority among all 13 vulnerabilities identified.

Views varied as to which part of the financial sector was impacted; NL noted it as prevalent in the whole financial sector and SI said that it was important for all entities dealing with financial markets, where those entities are heavily reliant on IT services provided by third parties or outsourcing firms, while RO said it was an issue for financial market infrastructures and critical participants.

Many Member States expressed concern over insufficient control over third parties. This concern specifically related to the cybersecurity of IT assets managed by third parties, which was raised by a number of Member States (DE, LT, IT). ES noted that an effective update of the risk controls, as a result of the increased number and criticality of IT services outsourced by credit institutions, is not performed. Consequently, an institution's IT risk profile is not always maintained within its IT risk appetite. Other risk control issues expressed were where credit institutions export data to unregulated third parties, which provide services on their behalf (ES), and difficulties to ensure control measures in the case of intragroup outsourcing (HU).

The lack of governance over outsourcing was identified for many firms in IE, in particular for smaller institutions. There is a lack of adequate oversight due to limited resources (MT), which may have an impact on the continuous provision of services and activities (SI). IE also pointed out that the risk assessment for the use of third parties has some fundamental errors as, quite often, the risk assessment for outsourcing is based on the monetary spend of the contract rather than on the risk of the service delivered.

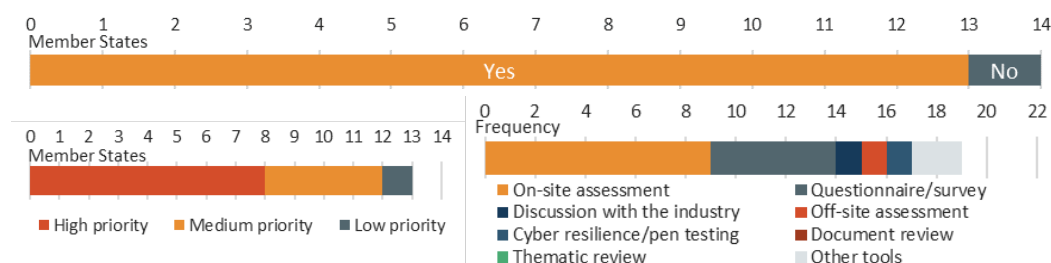
Other identified issues include:

- insufficient auditing of third-party contracts by the outsourcing institutions (BE);
- concerns over the content of contracts: (i) the increase of outsourcing (also in the form of cloud computing) for critical processes and institutions, especially by smaller institutions, which often lack the bargaining power to negotiate better contracts (BE); or (ii) the contracts frequently lack relevant clauses (e.g. requirements for sub-contracting or incident reporting) (ES); and



- concentration risk for some IT services (such as cloud or mainframe providers) (ES).

Chart A.4
Inadequate cyber hygiene



This is the second highest priority vulnerability for respondents. Views varied as to the types of institutions impacted; NL and SI consider that it is mainly an issue for smaller institutions, while RO noted it as an issue for financial market infrastructures and critical participants.

Some specific cyber hygiene issues mentioned by respondents include:

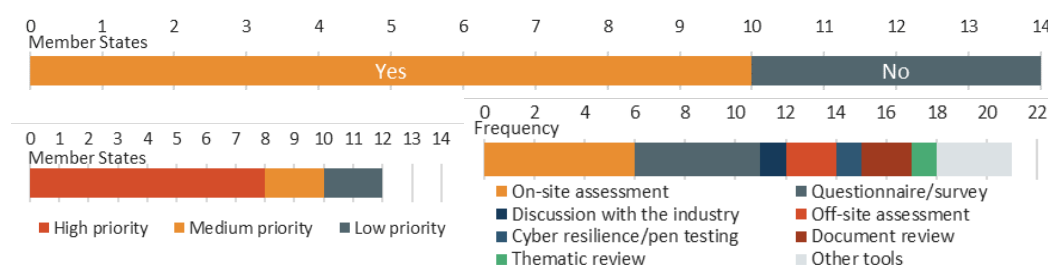
- the quality and completeness of some asset inventories (BE);
- vulnerabilities of IT systems not fixed in due time, and access rights may be misused and/or the misuse may not be identified (DE);
- there is no guarantee that known vulnerabilities have been fixed or security patches are applied at all or in a timely manner for all of the affected IT assets (ES);
- poor patching cycles with months between identifications and remediation, or usage of network protocols with known vulnerabilities (IE and PL);
- weaknesses in anti-malware protection (such as the lack of anti-malware in Unix systems) (ES);
- incomplete asset inventory which limits the institution's understanding of its perimeter, extent of exposure and/or internal propagation channels;
- difficulties for user access management processes to ensure that "least-privilege" and "need-to-know" principles⁷² are applied; lack of synchronisation between physical and logical security (ES);
- lack of proper asset management, rendering it impossible to guarantee the configuration of the correct items (IT).

⁷² These refer to the practices of limiting access rights for users to the bare minimum permissions they need to perform their work.



Chart A.5

Ineffective testing of people, processes and technology



This vulnerability was ranked third in terms of priority. Testing of people, processes and technology is considered an essential part of cyber risk management. However, the vulnerability is that the sector does not conduct this adequately in a cyber risk context. There were various views as to which types of institutions are most affected by this vulnerability. NL views it as a concern for the whole financial sector, while PL sees it mainly as an issue for some medium-sized and small banks, SI as an issue for small banks and RO as an issue for financial market infrastructures and critical participants.

Some respondents already have some cyber-related testing under way. For example, since 2016 BE has required its systemically important institutions to organise red-team exercises⁷³ on a regular basis to test their detection and response capabilities. In IT, although tests are usually performed in the context of disaster recovery planning, they tend to be focused on the restoration of IT assets; scenarios do not consider the data integrity impacts associated with scenarios involving malicious cyber incidents. In MT, the assessment of cybersecurity risks is typically conducted as part of the audits carried out and if the scoping is performed well, these should also cover cyber risk.

In ES, there is no obligation to test, and detection mechanisms are only tested in the course of operations with real alerts. No tests check the effectiveness of the detection mechanisms outside the annual cyber exercises, which include institutions classed as critical infrastructure operators.

In IE, institutions conduct internal cyber awareness exercises, such as internal phishing campaigns, rather than testing. HU found that this vulnerability is not specifically relevant, as most large institutions conduct cybersecurity testing and exercises, while smaller organisations are less relevant from a systemic point of view.

⁷³ Also known as “threat-led penetration testing”. A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity’s people, processes and technology, with minimal foreknowledge and impact on operations.



Annex 2: Overview of other relevant studies

The conceptual systemic cyber risk model developed by the ESCG adds to a growing body of work on the systemic dimensions of cyber risk. Cyber risk has been featured as a key risk in financial stability reports by various central banks, including the European Central Bank (2018a, 2018b, 2019), the Bank of England (2018), the Bundesbank (2019), De Nederlandsche Bank (2019), and Norges Bank (2019). As noted by Healey et al. (2018b), while no incidents to date have resulted in financial instability, the potential impact of a carefully timed malicious cyber incident designed to exploit the (negative) dynamics associated with traditional financial contagion channels has, so far, been insufficiently examined by academia, public authorities and the private sector. The ESCG's conceptual systemic cyber risk model attempts to bridge this gap.

A number of recent publications on systemic cyber risk reflect a growing acknowledgement of cyber risk as a potential trigger of financial instability. This is also reflected by the recent regulatory initiatives as highlighted in Section 2.2. The World Economic Forum (2016) offered one of the first definitions of systemic cyber risk: "the risk that a cyber event [...] at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security". The ESCG's conceptual systemic cyber risk model follows a similar logic, tracing a cyber incident from its point of origination to the impairment of key economic functions provided by the financial system, and ultimately to losses in the real economy. One additional element of the conceptual model, not explicitly captured in the WEF's definition, is the tipping point at which the impact exceeds the system's ability to absorb the shock. According to Kopp et al. (2017), cyber risk is a textbook example of systemic risk. The authors identify the main sources of systemic cyber risk as being access vulnerabilities, risk concentration and risk correlation, and contagion. Analysis by the Office of Financial Research (2017) suggests three channels through which cybersecurity events can threaten financial stability: lack of substitutability, loss of confidence, and loss of data integrity. Healey et al. (2018a) argue that at least one channel should be added to the three identified by the OFR, namely a lack of ICT substitutability. The authors point out that a large (and growing) percentage of the world's computing and storage falls to just a few cloud service providers; corporate IT enterprises tend to be extremely similar and run the same operating systems and applications; all companies depend on the same basic internet protocols, and local disasters often reveal unexpected physical dependencies by disrupting entire regions or industries. Healey et al. (2018a) identify three main differences between cyber and financial shocks that can create systemic instability: timing of incidents, complexity of cyber systems, and adversary intent. Kashyap and Wetherilt (2019) distinguish between shocks and impacts and discuss the respective roles for micro- and macroprudential regulation. Bouveret (2018) identifies patterns in cyber incidents and proposes a quantitative framework to assess cyber risk.

Similar to the ESCG's work, some publications include stylised scenarios to illustrate the systemic potential of cyber risk. The loss or compromise of the availability and integrity of financial data in key parts of the financial system is typically flagged as a key concern (World Economic Forum, 2016; Office of Financial Research, 2017; Institute of International Finance,



2017). Another recurring scenario involves a malicious cyber incident directed at a financial market infrastructure, leading to the failure or prolonged disruption of payment and settlement systems (World Economic Forum, 2016; Institute of International Finance, 2017). All scenarios cited involve a loss of confidence.

By contrast, Danielsson et al. (2016) argue that cyber risk is unlikely to be the (root) cause of a systemic crisis, but still draw conclusions that do not differ significantly from the findings in this report. While the authors argue that a cyber incident is extremely unlikely to trigger a systemic crisis, they also concede that in the presence of sufficient economic risk-taking by market participants and the “right” timing, a cyber incident could well act as a trigger for a systemic crisis. Indeed, it would need to be impeccably timed and coincide with non-cyber events that undermine confidence in the financial system. A key point of agreement between the analysis by Danielsson et al. and the analysis in this report is the importance of the confidence channel, as explored in Sections 3.2 and 3.3.

The Cambridge Centre for Risk Studies (2014) outlines how a hypothetical cyber incident could grow into a severe economic crisis with losses on a par with the 2007-08 global financial crisis. Their scenario describes how Sybil Corporation, a hypothetical systemically important technology enterprise, suffers an incident triggered by an insider that impacts its flagship database product. In the scenario, a disgruntled employee introduces a floating point error computation that appears randomly on a number of servers using Sybil's database product. As Sybil Corporation is a global ICT provider, the floating point error corrupts data integrity across a vast number of platforms, businesses and sectors. Once the cyber incident has been identified, panic spreads, as there is general uncertainty surrounding data quality and integrity, as well as uncertainty about which companies have been affected.

Depending on the latency period, the scenario is estimated to lead to a global recession lasting between six and 12 months and costing between USD 4.5 and 15 trillion (8-26% of global GDP). The floating point error is integrated into a routine upgrade of the Sybil software and thereby quickly spreads across the globe to all companies using Sybil's databases. The latency period between the commencement of the incident and its discovery is crucial in assessing the extent and impact of data corruption. The threat actor designs the floating point error so that it only appears when the last three digits of the server serial number match a specific number. As the error is hard to replicate and replacing corrupt servers appears to fix the issue, the incident can remain undetected for a prolonged period of time.

The discovery of the data corruption leads to general information malaise and mistrust in data. The corruption of data integrity has enormous ramifications for the global economy: products with faulty designs have been manufactured causing industrial malfunctions (e.g. oil spills, production line robot malfunction, corrupt semi-conductor production, etc.), erroneous automated investment decisions have been taken, accounting errors have been introduced into balances, etc. Once the cyber incident and its causes become known, businesses and customers alike do not trust their data anymore. Companies will take months to rebuild their databases and remove the corrupt data. Losses materialise from paying compensation, class actions and legal proceedings, and from shareholder and analyst reactions which result in a loss of value of the stocks of affected companies.



References

- Bank of England (2018), **“Could a cyber attack cause a systemic impact in the financial sector?”**, Quarterly Bulletin, 2018 Q4.
- Bouveret, A. (2018), **“Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment”**, IMF Working Paper No 18/143.
- Cambridge Centre for Risk Studies (2014), **“Sybil Logic Bomb Cyber Catastrophe Scenario”**.
- Danielsson, J., Fouché, M. and Macrae, R. (2016), **“Cyber risk as systemic risk”**.
- Duffie, D. and Younger, J. (2019), **“Cyber runs: How a cyber attack could affect U.S. financial institutions”**.
- De Nederlandsche Bank (2019), **“Financial Stability Report”**.
- Deutsche Bundesbank (2019), **“Financial Stability Report”**.
- European Central Bank (2018a), **“TIBER-EU framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming”**.
- European Central Bank (2018b), **“Cyber resilience oversight expectations for financial market infrastructures”**.
- European Central Bank (2019), **“ECB Banking Supervision: Risk Assessment for 2019”**.
- Healey, J., Mosser, P., Rosen, K. and Tache, A. (2018a), **“The future of financial stability and cyber risk”**, Brookings Institution.
- Healey, J., Mosser, P., Rosen, K. and Wortman, A. (2018b), **“The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability”**, CRFS Working Paper.
- Institute of International Finance (2017), **“Cyber Security and Financial Stability: How Cyber-attacks Could Materially Impact the Global Financial System”**.
- Kopp, E., Kaffenberger, L. and Wilson, C. (2017), **“Cyber Risk, Market Failures, and Financial Stability”**, IMF Working Paper No 17/185.
- Norges Bank (2019), **“Financial Stability Report”**.
- Office of Financial Research (2017), **“Cybersecurity and Financial Stability: Risks and Resilience”**.
- Ros, G. (2020), **“The making of a cyber crash”**, *ESRB Occasional Paper Series*, Forthcoming.
- Kashyap, A. and Wetherilt, A. (2019), **“Some Principles for Regulating Cyber Risk”**, AEA Papers and Proceedings, 109:482-487.
- World Economic Forum (2016), **“Understanding Systemic Cyber Risk”**, White Paper.



Imprint and acknowledgements

This report was approved by the ESRB General Board on 19 December 2019. It was prepared by the European Systemic Cyber Group, chaired by Paul Williams of the Bank of England under the auspices of the ESRB Advisory Technical Committee. Substantial contributions were made by:

Paul Williams (Chair)

Bank of England

Hannah Green

Bank of England

Greg Ros

Bank of England

Anne Wetherilt

Bank of England

Francisco Herrera

Banco d'España

Andrea de Vendictis

Banca d'Italia

Borut Poljsak

Banka Slovenije

Theresa Nabel

Bundesanstalt für Finanzdienstleistungsaufsicht

Tom Keating

Central Bank of Ireland

Maarten Willemen

De Nederlandsche Bank

Christoph von Busekist

Deutsche Bundesbank

Vaidotas Tamulenas

European Banking Authority

Nicola Yiannoulis

European Banking Authority

Emran Islam

European Central Bank

Wiebe Ruttenberg

European Central Bank

Claus Sengler

European Central Bank

Dinant Veenstra

EIOPA

Eleni Katsigianni

ESRB Secretariat

Pedro Marques

ESRB Secretariat

Tiago de Oliveira Bolhao Páscoa

ESRB Secretariat

Eric Schaanning (Secretary)

ESRB Secretariat

Gabriella Biró

Magyar Nemzeti Bank

Elise Vik Sætre

Norges Bank

Ylva Søyvik

Norges Bank

Aleksi Grym

Suomen Pankki – Finlands Bank

© European Systemic Risk Board, 2020

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.esrb.europa.eu

All rights reserved. Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged.

The cut-off date for the data included in this report was 19 December 2019.

ISBN 978-92-9472-131-0 (pdf)
DOI 10.2849/566567 (pdf)
EU catalogue No DT-04-20-113-EN-N (pdf)