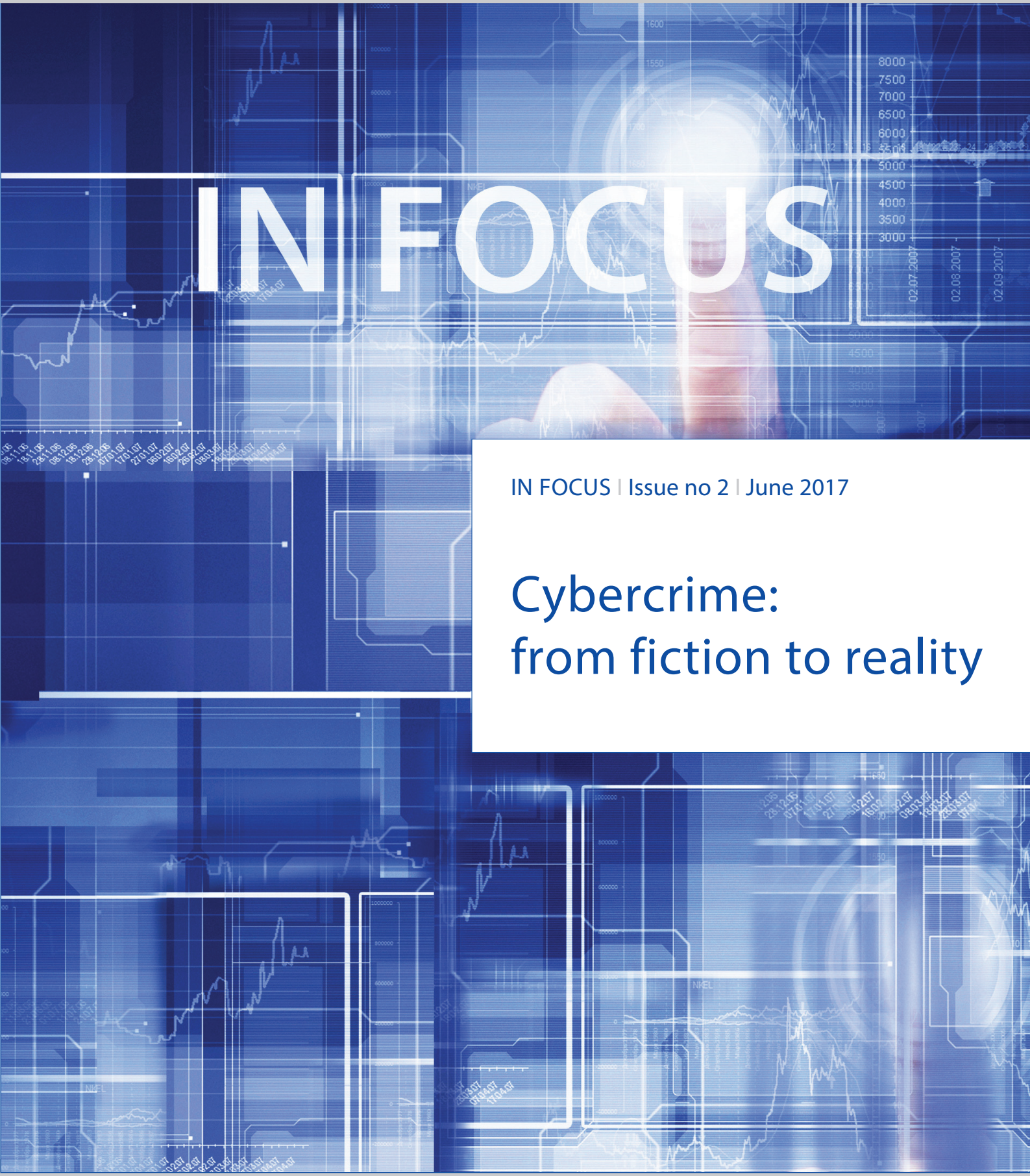
EUROPEAN CENTRAL BANK

EUROSYSTEM



IN FOCUS | Issue no 2 | June 2017

Cybercrime: from fiction to reality

EUROPEAN CENTRAL BANK

EUROSYSTEM

Cybercrime: from fiction to reality

Ensuring cyber resilience in financial market infrastructures in Europe

"All things change in a dynamic environment."

Introduction

Since the late 1980s digitalisation in communication and information technology has triggered significant social and economic changes worldwide. It has created a situation in which information, communication and commerce are no longer subject to the constraints of time and space. They can be accessed 24/7, instantaneously and at the global level.

To distinguish the concepts, products and services related to digital communication and information technology from their non-digital counterparts, prefixes and adjectives, such as “e” (e.g. email, ecommerce, ebook), “i” (e.g. iPhone, iTunes), virtual (e.g. virtual reality, virtual currency) and cyber (e.g. cybercrime, cybercop, cyberespionage, cyberwarfare) are widely used. Particularly the latter has become highly prevalent in popular culture, with cyborgs (short for cybernetic organism), cyber men and cyber killers populating manga, films and novels. Cyber Monday has become one of the biggest online shopping days of the year, and there is talk of cyber cities, cyberworld, cyberspace …

As with many things in life, there are two sides to the sheer endless possibilities of cyber reality. While digitalisation and globalisation have opened up new opportunities for individuals and companies to obtain information, conduct business and communicate, the increase in the number of users and amount of data on digital platforms, in cloud computing and across networks has also created more potential channels for criminal attacks. Crime never sleeps, and cybercriminals are always increasing their level of sophistication and exploring new opportunities for attack.

One motive is financial gain. For example, in 2013 online payment card fraud caused losses of almost €1 billion.[1] Owing to the virtual and international dimension of this crime, investigative measures are very complex.[2] For any investigation to be successful, law enforcement authorities in individual countries need to cooperate with each other and engage the help of all market actors concerned. In the case of payment card fraud, this means involving payment card schemes, banks, logistics companies and online merchants. However, for many of them, sharing information on security breaches that they have experienced is a sensitive issue and needs to be handled carefully.

As worrying as cyberattacks for financial gain are, there have been other troubling instances of cybercrime/cyberterrorism where attacks have focused on critical infrastructures, with the aim of bringing down the system, destroying data and damaging trust in the operator. For example, shortly before Christmas 2015, a

[1] To date, the ECB has published four reports on card fraud, highlighting that around two-thirds of card fraud within the Single Euro Payments Area (SEPA) results from card-not-present transactions, i.e. card payments via the internet, by post or by telephone. See www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

[2] See www.europol.europa.eu/newsroom/news/first-european-wide-action-e-commerce-fraud-sees-arrest-of-42

cyberattack on Ukraine's electricity infrastructure left 700,000 inhabitants of the south-western part of the country in the dark. Although it took just a few hours to restore power to all the affected areas, it took more than two months for the control centres of the infrastructure to become fully operational again.[3] It seems clear that the primary purpose of this attack was not financial gain, but to disrupt and destabilise the system, which makes attacks of that nature even more difficult to predict.

Perhaps unsurprisingly, there have also been cyberattacks with the aim of disrupting and destabilising the system at the same time as profiting financially. One example is the recent worldwide attack by WannaCry. In the afternoon of Friday, 12 May 2017, it became apparent that a new type of malware was quickly spreading across the internet and having a considerable impact on the machines it infected. The malware was a type known as "ransomware", in which the malware encrypts files on a computer or network and requires the owner of the computer system to pay a ransom in order to receive the key to decrypt the files. Within several hours, the WannaCry malware had infected over 45,000 machines in over 70 countries, and over the weekend of 13-14 May, the number of infected machines identified had increased to over 250,000 in over 150 countries. The impact was profound, affecting banks, transport networks and healthcare facilities.

It does not require a lot of imagination to envision the horror scenario following a cyberattack on a power grid involving nuclear power plants, or a cyberattack that brings transport networks and hospitals to a standstill. It may be less easy to envisage the damage of a cyberattack on a critical financial market infrastructure (FMI), but such attacks are equally daunting. Furthermore, according to the Federal Reserve Bank of New York, when it comes to an attack on an FMI, it is not a question of "if" but "when".[4]

This paper gives some insight into legislative and regulatory initiatives being carried out in the European Union (EU) and at the international level in order to increase cyber resilience and into the Eurosystem's strategy for ensuring cyber resilience in FMIs.

1 Legislative and regulatory response to cyberthreats at the European and international level

Given the increase in both the frequency and severity of cyberattacks in recent years, it is not surprising that legislators, regulators and international standard-setting bodies have issued legislation and guidance on cybersecurity at the national and international level, both cross-sector and sector-specific. The following sections

[3] See https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[4] See https://www.newyorkfed.org/newsevents/speeches/2016/dzi160503

briefly outline the different angles of legislative and regulatory initiatives that are particularly relevant for the Eurosystem's market infrastructure.

1.1 EU legislation on cybersecurity

Cybersecurity and digital privacy are high on the list of priorities of the European Commission.[5] In 2013 the Commission published its cybersecurity strategy, a comprehensive vision on how best to prevent and respond to cyber disruption and attacks.[6] In the same year, the European Cybercrime Centre (EC3) was established at the European Police Office (Europol) in The Hague to strengthen the law enforcement response to cybercrime in the EU.[7] To bring cybersecurity capabilities to the same level of development in all EU Member States and ensure that exchanges of information and cooperation are efficient, including at the cross-border level, the Commission adopted the Directive on security of network and information systems (the NIS Directive)[8] in July 2016. This Directive, which Member States are required to transpose into national law by May 2018, is the main legislative instrument supporting cyber resilience in the EU. It applies to operators of essential services, e.g. operators of ecommerce platforms, social networks and critical infrastructures, such as transport, energy, health and financial services, i.e. credit institutions and some FMIs. The key components of the NIS Directive are detailed in Box 1.

[5] See https://ec.europa.eu/digital-single-market/en/cybersecurity-privacy

[6] See http://europa.eu/rapid/press-release_IP-13-94_en.htm

[7] See https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[8] 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 (OJ L 194, 19.7.2016, p. 1).

For the cyber landscape in the EU, the adoption of the EU General Data Protection Regulation[9] in 2016 (which will apply from May 2018) is another major step forward. For the first time, companies across the EU will be required to disclose data breaches to national data protection authorities.

Box 1

Directive concerning measures for a high common level of security of network and information systems (NIS Directive)[10]

"The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;

- Cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to establish a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;

- A culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to report serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive."

1.2 International guidance on cybersecurity in the financial sector

Public authorities have recognised that the interconnectedness of the global financial system requires a strategically aligned approach to cybersecurity at the international level. Hence, the members of the G7 (i.e. Canada, France, Germany, Italy, Japan, the United Kingdom, the United States and the EU) set up a Cyber Expert Group that was tasked with identifying the key cybersecurity risks for the financial sector across the G7 and proposing recommendations for further work in this field. The recommendations included developing the G7 fundamental elements of cybersecurity. Three further recommendations on the effectiveness of cybersecurity assessments, third-party risks and coordination with other critical sectors have also been endorsed by the G7.

[9] 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) (OJ L 119, 4.5.2016, p. 1).

[10] Quoted from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

The “G7 fundamental elements of cybersecurity for the financial sector” were published in October 2016 and are intended to be non-prescriptive and non-binding, providing each jurisdiction within the G7 (and beyond) with the flexibility to align domestic strategies as deemed appropriate. The European Central Bank (ECB) contributed to the development of the fundamental elements, welcomes their adoption by the G7 finance ministers and central bank governors, and encourages all jurisdictions to work on adopting them.

The G7 report is intended to provide high-level guidance to support financial entities in creating cybersecurity strategies and policies. Its key elements are listed in Box 2. The G7 is currently working on the implementation of the three remaining recommendations.

Box 2

G7 fundamental elements of cybersecurity for the financial sector[11]

1. Cybersecurity Strategy and Framework: Establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines.

2. Governance: Define and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability; and provide adequate resources, appropriate authority, and access to the governing authority (e.g. board of directors or senior officials at public authorities).

3. Risk and Control Assessment: Identify functions, activities, products, and services – including interconnections, dependencies, and third parties – prioritise their relative importance, and assess their respective cyber risks. Identify and implement controls – including systems, policies,

[11] See https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5

procedures, and training – to protect against and manage those risks within the tolerance set by the governing authority.

4. Monitoring: Establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

5. Response: Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and customers as appropriate); and (d) coordinate joint response activities as needed.

6. Recovery: Resume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.

7. Information Sharing: Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defences, limit damages, increase situational awareness, and broaden learning.

8. Continuous Learning: Review the cybersecurity strategy and framework regularly and when events warrant – including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components – to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

1.3 Specific guidance on cybersecurity in FMIs

Focusing on financial stability, the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) have sought to understand the cyber risks faced by FMIs and the level of readiness of FMIs to deal with worst-case scenarios effectively. The report on “Cyber resilience in financial market infrastructures” of November 2014[12] analyses the relevance of cybersecurity issues for FMIs and their overseers in the context of the “Principles for financial market infrastructures” [13].

In June 2016 CPMI-IOSCO published principle-based “Guidance on cyber resilience for financial market infrastructures”.[14] As summarised[15] in Box 3, this guidance, which aims to enhance cyber resilience in FMIs, outlines five primary risk management categories (i.e. governance, identification, protection, detection, and

[12] See http://www.bis.org/cpmi/publ/d122.htm

[13] See https://www.bis.org/cpmi/publ/d101a.pdf

[14] See http://www.bis.org/cpmi/publ/d146.pdf

[15] See the CPMI-IOSCO “Guidance on cyber resilience for financial market infrastructures”.

response and recovery) and three overarching components (testing, situational awareness, and learning and evolving) that should be addressed across FMIs' cyber resilience frameworks. In so doing, it does not aim to introduce new standards, but rather to elaborate on the principles which are already established in the "Principles for financial market infrastructures".

Box 3

Primary risk management categories and overarching components to be addressed across an FMI's cyber resilience framework

Governance: Effective governance should start with a clear and comprehensive cyber resilience framework. Such a framework should be guided by a cyber resilience strategy, define how the FMI's cyber resilience objectives are determined and outline its people, processes and technology requirements for managing cyber risks. It is essential that the framework is supported by clearly defined roles and responsibilities of the FMI's board (or equivalent) and its management, and it is incumbent upon its board and management to create a culture which recognises that staff at all levels, as well as interconnected service providers, have important responsibilities in ensuring the FMI's cyber resilience.

Identification: Given that FMIs' operational failure can negatively impact financial stability, it is important that FMIs identify their critical business functions and supporting information assets that should be protected, in order of priority, against compromise.

Protection: Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of FMIs' assets and services. FMIs are urged to implement appropriate and effective controls and to design systems and processes in line with leading cyber resilience and information security practices to prevent, limit and contain the impact of a potential cyber incident.

Detection: An FMI's ability to detect the occurrence of anomalies and events indicating a potential cyber incident is essential to strong cyber resilience. Early detection provides an FMI with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches. Given the stealthy and sophisticated nature of cyber attacks and the multiple entry points through which a compromise could take place, advanced capabilities to extensively monitor for anomalous activities are needed.

Response and recovery: Financial stability may depend on the ability of an FMI to settle obligations when they are due, at a minimum by the end of the value date. Therefore, an FMI's arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them. Continuity planning is essential in meeting related objectives.

Testing: Once employed within an FMI, the elements of its cyber resilience framework should be rigorously tested to determine their overall effectiveness. Sound testing regimes produce findings that should be used to identify gaps against stated resilience objectives and provide credible and meaningful inputs to the FMI's management of cyber risks.

Situational awareness: Strong situational awareness can significantly enhance an FMI's ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyberattacks that are not prevented. Specifically, a solid understanding of the threat landscape can help an FMI to better identify and understand the vulnerabilities in its critical business functions, and facilitate the adoption of appropriate risk mitigation strategies.

Learning and evolving: To enable efficient management of cyber risks, it is important to implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks. FMIs should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organisation.

It should be noted that FMIs are not viewed as stand-alone entities. Given the extensive interlinkages and interdependencies in the financial system, it is understood that the markets' overall cyber resilience depends not only on the resilience of each individual FMI, but also on that of interconnected FMIs, of their participants and their service providers.

The guidance is intended not only for FMIs but also for overseers, supervisors and authorities, making it clear that the response to cyber risk must be a collective and united effort. Cooperation is vital to ensure consistency in the direction and application of oversight and supervisory practices with regard to both FMIs and their respective participants.

With the publication of the guidance, FMIs were required to "immediately take necessary steps in concert with relevant stakeholders to improve their cyber resilience […]. In particular, they should also, within 12 months of the publication of the guidance, have developed concrete plans to improve their capabilities in order to meet the two-hour RTO", i.e. the objective of enabling the safe resumption of critical operations within two hours of a disruption.[16]

2 Developing a Eurosystem strategy for cyber resilience in FMIs

Following the financial crisis of 2007-08, legislators and international standard-setting bodies focused primarily on legislation and standards aimed at improving risk management, recovery and resolution. Against the backdrop of the rising number of cyberattacks on the financial sector, it has become clear that on top of the "traditional" risk management, IT security and business continuity measures to protect operations from critical failures, FMIs need to find new ways of ensuring resilience against cyberattacks. Cyber resilience goes beyond technology, as it also encompasses governance, company culture and business processes. Accordingly, overseers must adapt and evolve their oversight approaches and techniques, taking

[16] See the CPMI-IOSCO "Guidance on cyber resilience for financial market infrastructures", p. 3.

into account cyber risk as well. A paradigm shift is crucial and a cyber resilience strategy is needed.

In recognition of the escalating cyberthreats, the legislative and regulatory guidance and the required paradigm shift, the Eurosystem's overseers have launched a strategy for cyber resilience in FMIs.

The aim of the strategy, which was approved by the Governing Council of the ECB in April 2017, is to improve the cyber resilience of the EU's financial ecosystem by enhancing individual FMIs' readiness and by fostering sectoral resilience and collaboration, in the context of increasing interdependencies, vulnerabilities and threats.

The strategy is built on three pillars, which are shown in Figure 1. The following sections elaborate further on these three pillars.

Figure 1
Pillars of the Eurosystem's strategy in relation to FMIs

Source: ECB.

2.1 Pillar 1: FMI readiness

In order to ensure that the CPMI-IOSCO "Guidance on cyber resilience for financial market infrastructures" discussed in Chapter 1 is put into practice in a consistent manner, the Eurosystem is implementing a harmonised approach to assessing payment systems in use in the euro area against the Guidance. In addition, it is

developing a range of tools that can be used by FMI operators to enhance their cyber resilience maturity.

One of these tools includes the development of a “European Red Team Testing Framework” (hereinafter referred to as the “Testing Framework”). The term “red-team testing” is originally a military term used to describe a team tasked with penetrating the security of “friendly” installations, and thus testing their security measures. In the context of cyber resilience, it is an exercise which mimics the tactics, techniques and procedures of real attackers, based on bespoke threat intelligence, and seeks to target the people, processes and technologies of an FMI or firm, in order to test its protection, detection and response capabilities without prior warning. The red team test is regarded as one of the most comprehensive ways to test cyber resilience.

The forthcoming Testing Framework was inspired by similar initiatives in the United Kingdom, the Netherlands, Hong Kong and Singapore. Its aim is to ensure standardisation and mutual recognition of cyber testing across the EU, thereby avoiding FMIs being subject to tests in/by every EU Member State. A key element of effective cyber resilience is to encourage multi-jurisdictional, group testing that is recognised by different authorities and to ensure a certain level of efficiency for FMIs.

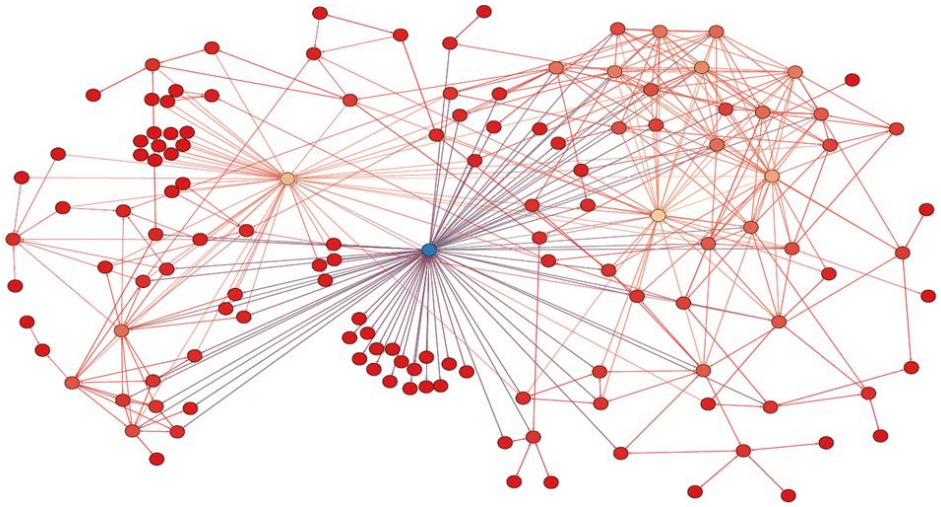
Furthermore, the Testing Framework aims to raise the standards of cyber testing by establishing standards for penetration testers and threat intelligence providers, to catalyse accreditation at the EU level and to help the market to access the best and most reliable testers for their critical infrastructures.

2.2 Pillar 2: Sector resilience

Cyber resilience in an FMI depends not only on its own readiness, but also on that of its participants, service providers and interconnected FMIs. There is a broad range of entry points through which an FMI could be attacked, e.g. via participants, service providers, vendors and vendor products, and linked FMIs. The FMI itself could even become a channel for propagating cyberattacks, e.g. by inadvertently distributing malware to other FMIs. From a cyber perspective, a small-value/volume participant or a vendor providing non-critical services may be as risky as a major participant or a critical service provider. The high degree of interconnectedness within the ecosystem necessitates strong cyber resilience across the sector all the more.

The FMI sector map in Figure 2 illustrates how the FMIs in the EU are linked, as well as the extent of the interconnectedness and interdependencies in the EU financial system, with a plethora of stakeholders.

Figure 2
FMI sector map



Source: ECB
Note: The sector map, which has been anonymised for ease of display, includes all the FMIs in the EU, and how they are linked to each other.

In order to strengthen the sector's cyber resilience, it is important to understand the operational interdependencies through sector mapping, foster cross-border and cross-authority collaboration, establish effective information-sharing and implement market-wide business continuity exercises.

Sector mapping and the identification of critical nodes will deepen the knowledge of cross-market dependencies, supply chains and third-party involvement. The Eurosystem's overseers are currently developing an analytical framework and methodology for sector mapping. The aim is to produce a number of sector/network maps that will be used to understand key risk areas, improve crisis communication procedures, enhance information-sharing and debate other policy issues.

With regard to collaboration, cross-border, cross-authority collaboration needs to be enhanced to avoid different levels of cyber resilience maturity within the financial sector and to ensure that authorities adopt similar approaches and focus on similar priorities. To counter the risk of fragmentation, it is vital to foster cooperation on cyber resilience between the appropriate authorities at both the European and the national level, particularly because different authorities have their own separate mandates for the various types of FMI and financial institution.

Another key component of sector-wide cyber resilience is the efficient sharing of information on threats between market participants, between market participants and regulators, and between regulators. There needs to be a strategy for overcoming the current fragmentation in the European information-sharing landscape, as well as a mind shift to move beyond incident reporting towards also sharing ex ante operational, tactical and strategic threat intelligence. The Eurosystem is currently

exploring information-sharing arrangements, with a view to streamlining procedures to the benefit of all stakeholders in the ecosystem.

Currently, there is a significant focus on protecting against and detecting cyberattacks. However, the cornerstone of effective resilience is to acknowledge that an attack is imminent, and all infrastructures must be in a position not only to withstand such attacks, but also to respond in an appropriate way and recover in a safe and efficient manner. To further enhance the readiness of FMIs, market-wide exercises and cyber simulations are key.

ENISA, the European Agency for Network and Information Security, is the first entity to conduct EU-level cyber incident and crisis management exercises for both the public and private sectors in the EU and EFTA Member States. The Cyber Europe exercises are simulations of large-scale cybersecurity incidents that escalate into cyber crises. The exercises offer opportunities to analyse advanced technical cybersecurity incidents and deal with complex business continuity and crisis management situations.[17]

With regard to specific exercises for FMIs, the TITUS exercise, which was a crisis communication exercise involving euro area FMIs, was carried out in 2015 and was the first of its kind.[18] In line with the strategic aim of sectoral cyber resilience, setting up such exercises on a recurrent and more consistent basis should allow FMIs to build up their knowledge of and expertise in handling potential threat situations.

2.3 Pillar 3: Strategic regulator-industry engagement

The EU recognises the importance of establishing a forum which brings together market actors, competent authorities and cybersecurity service providers. A number of Member States[19] are leading the way, having established formal public-private partnerships or industry associations for cybersecurity. However, there is no pan-European equivalent at present.

The sector mapping discussed above will not only identify the critical nodes in the EU financial system, but also help to pinpoint those market participants and regulators that should be involved in a pan-European regulator-industry forum. Such a pan-European forum should ensure Board-level participation and focus on strategic discussions rather than overly technical details, as well as aim to raise awareness and catalyse joint initiatives for developing effective solutions for the market, sharing best practices and fostering trust and collaboration. Moreover, as mentioned under second pillar, information-sharing between relevant stakeholders is

[17] For more information, see www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

[18] See www.ecb.europa.eu/pub/pdf/other/crisis_communication_exercise_for_euro_area_financial_market_infrastructures.en.pdf

[19] Austria, Belgium, Denmark, France, Germany, Italy, the Netherlands, Spain, Sweden and the United Kingdom.

an important component of the Eurosystem's strategy, which could be enhanced through collaboration within the pan-European forum. Tackling cyber risk is not for regulators or the market in isolation, but is an endeavour that they must undertake together.

3 Conclusion

Going forward, it is important that governments/government agencies, public authorities, committees and market actors adopt a joint approach to ensuring cyber resilience. This will facilitate cross-fertilisation and collective learning. Cyber risk is no longer just an issue for technicians, it is a risk to the business itself and therefore a key item on the agenda of the management boards of market actors. Monitoring and detecting cyberattacks, disclosing breaches and disseminating cyberthreat intelligence in a timely manner and with a reasonable balance between privacy considerations and liability protection is the only way for businesses and FMIs to adapt, survive and flourish in the cyberworld.

In recognition of the escalating cyberthreats, the legislative and regulatory guidance and the required paradigm shift, the Eurosystem – in its capacity as overseer – is implementing the three pillars of its strategy for cyber resilience in FMIs. This strategy is not cast in stone. Since "all things change in a dynamic environment", it too needs to have the scope to continuously evolve in the light of new developments and lessons learned.

Cybercriminals are always coming up with more sophisticated ways to attack. Protection from cybercriminals can be only achieved if it is widely recognised that maintaining and improving cyber resilience in FMIs is the joint responsibility of regulators and industry across borders, from the top level down to individual participants, clients and employees.