CNMV
Comisión Nacional del Mercado de Valores

# Cyber security in market infrastructures

# Cyber security in market infrastructures

March 2017

Comisión Nacional del Mercado de Valores
Edison, 4
28006 Madrid

Passeig de Grácia, 19
08007 Barcelona



ISBN (digital edition): 978-84-87870-99-6

Layout: Composiciones Rali, S.A.

# Contents


| | | |
|---|---|---|
| Executive summary | | 7 |
| 1 | Definitions | 9 |
| 2 | International perceived risk of a cyber attack on market infrastructure | 11 |
| 3 | Organisational structure of cyber security in Spain | 13 |
| 4 | Directive (EU) 2016/1148 | 19 |
| 5 | Regulations applying in Spain | 21 |
| 6 | Work on cyber security by the Bank for International Settlements' Committee on Payments and Market Infrastructure | 23 |

# Executive summary

Market trading and post-trade infrastructures are seen as critical to cyber security by all countries including Spain. A cyber attack targeting a market's post-trade infrastructure (repositories, settlement and central counterparty) could trigger major and long-lasting systemic events which would be slower to reverse and recover from than an attack on trading systems.

The associated technology and interoperability of market infrastructures with other linked systems and with members offer cyber attackers not only routes to propagate and amplify their attacks but also potential entry points for threats.

Cyber security of critical infrastructure is a matter of national security for most countries, including Spain. International regulators such as IOSCO and industry bodies such as SIFMA have said that cyber security is one of their top priorities. This, coupled with the structural changes in the financial sector following the emergence and consolidation of the Fintechs, demands an urgent commitment of technology-capable human resources by supervisory bodies.

The nature of cyber threats is changing and continually evolving. Supervisory and regulatory responses need to be similarly fleet-footed. International cooperation and the sharing of data and experience (cyber intelligence) are key elements in the strategy to achieve greater security.

Market infrastructure bodies have to comply with cyber security requirements imposed by national competent bodies in the field and in securities markets and, specifically:

– The Financial Sector Strategic Plan developed by the National Committee for the Protection of Critical Infrastructure (CNPIC), containing the main recommendations of a working group on the issue, in which the CNMV took part. The plan should, among other points, contain CPSS-IOSCO's cyber security recommendations for infrastructure bodies. At European level, there is already a cyber security directive[1] covering infrastructures which is due to be transposed into national law by May 2018.

– Guidance[2] published by the BIS Committee on Payments and Market Infrastructure (CPMI) in June 2016. This will apply to market infrastructures and

1 Directive (EU) 2016/1148 of June 2016 concerning measures for a high common level of security of information networks and systems across the Union: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

2 "Guidance on cyber resilience for financial market infrastructures" Committee on Payments and Market Infrastructures. June 2016.

the CNMV will be responsible for supervising compliance in coordination with other cyber security agencies.

The CNMV will have to closely follow developments in CNPIC's action on critical infrastructure and cyber security, carrying out whatever supervisory tasks the corresponding plans assign us.

Periodic cyber attack exercises and simulations are an essential tool, and already regular practice in other countries. They should also be run in Spain for the infrastructure institutions overseen by the CNMV. Contingency plans for market infrastructures should include high-level external security audits on a periodic and permanent basis. The above-cited Committee on Payments and Market Infrastructure (CPMI) report can provide guidance for the supervision of cyber security policies in our markets. At EU scale, the European Union Agency for Network and Information Security (ENISA) has already run a number of exercises and simulations.

For cyber-security plans to be as effective as possible, it is essential to ensure participation by management and all employees of the firm as any workstation with an outside connection can be a potential entry point for cyber threats.

# 1 Definitions

This report uses the following concepts from the CPMI's "Guidance on cyber resilience for financial market infrastructures"[3] published in June 2016:

– Cyber threat: a circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a financial market infrastructure's systems, resulting in a loss of confidentiality, integrity or availability.

– Cyber resilience: the ability to anticipate, withstand, contain and rapidly recover from a cyber attack.

– Cyber security: this is a very general concept with no consensus definition. In this document it is used to mean strategies, policies and standards designed to reduce threats and vulnerabilities, including dissuasion, international commitments and attack response, resistance and recovery as well as the security policies applied by market infrastructure firms.

– Cyber intelligence: collection and analysis of data that allows infrastructure bodies to understand and mitigate the impact of cyber threats.

3 http://www.bis.org/cpmi/publ/d122.pdf

# 2 International perceived risk of a cyber attack on market infrastructure

Most supervisors and international organisations have recognised the risk posed to the financial system by a cyber attack on critical market infrastructure. Some have set in train various initiatives in response, ranging from round-table meetings to industry consultation and working groups.

In July 2015 IOSCO's secretary general[4] spoke of potential cyber attacks as one of the chief concerns for securities supervisors and one where risks were set to increase as markets relied ever more heavily on digital technology. IOSCO has set up a cyber security working group. In November 2015 it published an initial draft report followed by guidance in June 2016, setting out a number of principles that market infrastructure managers should follow. We comment on this in section 6.

In October 2015, the US Federal Reserve joined the derivatives market supervisor (CFTC) in declaring that the risk of cyber attacks was top of its list of priorities[5]. The Securities and Exchange Commission (SEC) hosted a round table in 2014 with various discussions [6] dedicated to cyber security.

Again in the US, the CFTC published a consultation document in 2015 "Proposed Enhanced Rules on Cyber security for Derivatives Clearing Organizations, Trading Platforms, and Swap Data Repositories". This report seeks to beef up existing standards and identifies five essential types of cyber security test: vulnerability, penetration, controls, incident response and technology risk assessment. How frequently these tests should be run will depend on the type of entity concerned and the equipment being tested. They can be done by independent firms specialising in cyber security. Since October 2016, these tests have become standard for all central counterparties and trade repositories. Another of the report's aims, echoing IOSCO's recommendations, is the involvement of firms' management bodies in security policies to counter cyber attacks.

The UK has a three-pronged initiative involving the Treasury, Bank of England and Financial Conduct Authority (FCA) that seeks to provide and compile data to ensure the resilience and continuity of the financial sector[7]. A UK government framework

4 http://www.bloomberg.com/professional/blog/cyber-risk-is-next-black-swan-uneven-across-the-globe-says-ioscos-medcraft/?utm_source=SmartBrief&utm_medium=SBRC&utm_content=Cyber-Risk%20Is%20%E2%80%98Next%20Black%20Swan%2C%E2%80%99%20Uneven%20Across%20the%20Globe%2C%20Says%20Iosco%E2%80%99s%20Medcraft&utm_campaign=Core

5 http://www.thinkadvisor.com/2015/10/14/fed-says-cybersecurity-is-right-at-the-top-of-prio

6 http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt

7 http://www.bankofengland.co.uk/financialstability/fsc/Pages/default.aspx

document[8] published in June 2014 sets out 10 key principles that firms' should consider to safeguard their cyber security. The FCA's business plan 2015-16 envisages coordination with the Bank of England, Treasury and Prudential Regulation Authority to evaluate the cyber resilience of critical infrastructure in the financial sector. The Bank of England's Financial Policy Committee saw cyber security threats as a key risk in for 2015 and warned of the need to run assessments of critical infrastructures.

In the Financial Stability Board (FSB) meeting of September 2015 in London, several members highlighted the potential threat to financial stability from cyber attacks.

8 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

# 3 Organisational structure of cyber security in Spain

Since 2013 Spain has had in place a Strategy Cyber Security plan drawn up by the Council for National Security. The plan sets the following objectives:

1. To ensure that the information and telecommunications systems used by the public sector have an adequate level of cyber security and resilience.

2. To develop security and resilience in the information and telecommunications systems used by the corporate sector in general and critical infrastructures in particular.

3. To build up capabilities in prevention, detection, reaction, analysis, recovery, response, investigation and coordination in response to terrorist and criminal activities in cyber space.

4. To raise awareness among Spanish citizens, professionals, companies and public sector bodies about the risks from cyber space.

5. To achieve and maintain the knowledge, skills, experience and technological capabilities that Spain needs to consistently meet all its cyber security objectives.

6. To help improve cyber security on an international scale.

One of the Plan's priorities for critical infrastructure is to improve the security of IT and telecommunications systems. To achieve this, it seeks to drive forward the implementation of standards (see section 5) on protection of critical infrastructure and capabilities to protect essential services.

The Plan prescribes the following cyber security structure for Spain:

a) Council for National Security: The Council for National Security, a government delegated committee, advises the President of the Government on National Security Policy.

b) Specialist Cyber Security Committee: The Specialist Cyber Security Committee supports the National Security Committee in its work and, particularly, advises the President on the direction and coordination of cyber security aspects of National Security Policy. It also fosters coordination, collaboration and cooperation between the various branches of government and public and private sector as well as supporting decision-taking in the Council itself with analysis, research and proposals of initiatives at national and international level.

c) Specialist Situation Committee: The Specialist Situation Committee is convened to manage cyber security crises whose reach, scale and impact go beyond the capabilities of the usual mechanisms.

Financial market infrastructures are counted as critical infrastructure within this system. Several institutions have been set up to coordinate and supervise cyber security preventative action and response. That said, the CNMV retains its supervisory duties over financial market infrastructure including over cyber security policy and procedures.

## Planning and organisation of cyber security for Spain's critical infrastructure

Spain has had a National Critical Infrastructure Protection Plan since 2007, which is classified. It was recently updated following the State Secretariat for Security's instruction 01/2016 of 10 February.

The main bodies charged with keeping Spain's critical infrastructure safe are:

– The National Commission for the Protection of Critical Infrastructure (PIC Commission), a collegiate body reporting to the State Secretariat for Security. The Commission has several members and is chaired by the Secretary of State for Security. Ministries included in the system's scope are represented by officials of director general rank or above.

– The National Centre for the Protection of Critical Infrastructures (CNPIC), reporting to the State Secretariat for Security.

The CNPIC steers, coordinates and supervises all the responsibilities of the Interior Ministry's State Secretariat for Security as regards protection of Spain's critical infrastructure.

Law 8/2011[9], of 28 April, establishing measures to protect critical infrastructure, defines critical infrastructure as: *strategic infrastructure (i.e. infrastructure that provides essential services) whose functioning is indispensable and for which there are no alternative solutions, such that its disruption or destruction would have a severe impact on essential services.* In the case of the financial sector, these are summarised in Law 44/2002, of 22 November, on Measures to Reform the Financial System.

The Secretariats of State for Security and for Telecommunications and the Information Society reached an agreement in 2012 (ratified in 2015) which, among other measures, set the framework for cooperation between the CNPIC and the National Cyber Security Institute on incidents affecting critical infrastructure located in Spain. In 2014, the State Secretariat for Security, set up the Cybernetic Coordination Office reporting to the CNPIC[10] with a brief to act as technical coordinator on cyber security issues and liaison point for national and international authorities.

9 https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

10 http://www.academiauniform.es/mediapool/81/814638/data/2014/Instrucc._15_14_Oficina_coordinacion_cibernetica.pdf

Both agencies have set up a response team specialising in analysis and management of technological security incidents. The response team is now the specialist centre for managing incidents affecting critical infrastructure in Spain.

If any critical infrastructure suffers a cyber security problem, its operator can call in the response team by reporting the incident through a single contact point.

Cyber exercises have been run[11] at both national and European scales, coordinated by the European Union Agency for Network and Information Security (ENISA https://www.enisa.europa.eu/), with thirty-two countries taking part. Exercises are run every two years[12]. The key conclusions drawn from the four exercises carried out since 2010 are, first, the need to develop a mechanism to share experiences of cyber attacks and best practice for improving cyber security and, second, to continue running regular exercises to a pre-set timetable.

A cyber security problem is defined as any incident that by using or targeting technological equipment affects the smooth running of the infrastructure affected, such as attacks that halt or render useless technological services, access to insider information, changes in information to fraudulently manipulate technological systems and the data they process, etc.

We were unable to get any information on the standards, procedures and tests run by CNPIC to safeguard infrastructure defined as critical, all of which are officially secret.

In 2016, results were released of a simulation run in September 2015 by the US Security Industry and Financial Markets Association (SIFMA), whose main conclusion was that, despite progress, further effort needs to be made on cyber security measures. More than 650 institutions took part in the exercise, including, besides financial institutions, US government agencies such as the Treasury Department, FBI, National Security Agency and various federal regulators. The exercise included a theoretical shutdown of a central counterparty and attacks on securities markets and multilateral trading facilities. SIFMA has published its strategic priorities for 2016, which put cyber security top of the list. In December 2015, the US Congress passed the Cyber Security Information Sharing Act[13] which allows companies and federal bodies to share their information on cyber attacks and best practice in this area.

## Cyber security and the CNMV

The following risks fall within the scope of the CNMV's responsibilities:

11 A cyber exercise is a tool that allows operators to gauge the state of preparedness of market participants for a cyber crisis, draw lessons and make recommendations for the future: improvements when faced with cyber attack, ways to improve cooperation and coordination between affected sectors, identification of interdependencies, improved awareness and training: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/incibe_taxonomia_ciberejercicios.pdf

12 "The 2015 Report on National and International Cyber Security Exercises Survey, Analysis and Recommendations". ENISA.

13 https://www.congress.gov/bill/114th-congress/senate-bill/754

– Issuers/listed firms. With different scopes of impact on business continuity and knock-on effects for the market. Especially severe in its impact would be a cyber attack on firms providing strategic and critical infrastructure such as electricity and communications, air traffic control or payment systems.

– Investment services companies, fund managers and depositaries. Impacting record-keeping of customers' securities and cash accounts.

– The supervisor itself: With especially critical processes, such as the dissemination of market relevant information, which could affect the market's functioning.

– Important financial information providers.

– Financial market infrastructures: trading, clearing and settlement, central counterparties and securities registers. These infrastructures are especially vulnerable to the risks of cyber attack as a result, first, of their heavy reliance on technology – all clearing and settlement now depends on IT – and, second, the deep interconnectedness of their members, which offers multiple potential ways of entry into their systems.

In this environment, we need to distinguish between the impact and reach of an attack on trading infrastructure and the consequences of an attack on post-trade infrastructure.

An attack on trading infrastructure would be immediately spectacular and significant if it succeeded in bringing down or disrupting trading. However, any systemic effects could be rapidly put right.

A penetration of post-trade infrastructures, however, could potentially have more serious consequences for financial stability if it successfully blocked settlement, clearing and central counterparty functions. Another potentially very harmful consequence for post-trade infrastructures would be the breach of trade data, which would confer significant advantages on anyone illicitly accessing insider information on open positions and the portfolios of other financial institutions.

It should be stressed that an article published by The Economist in November 2015[14] claims that the average time elapsing between a network being attacked and its owner becoming aware of the fact is 205 days. Market integrity would be under threat all this time if an attacker could access confidential information filed in trade repositories, central depositaries and central counterparty records. For this reason, analyses and penetration tests play a critical role in early detection of attacks which could compromise the confidentiality of central registers and result in leaks of insider information.

It would be useful to analyse new trends in systems and/or trading strategies (algorithmic trading) and securities clearing and settlement (distributed ledger technology, blockchains) to see if they reduce or actually increase the possibility of cyber attacks.

14 http://www.economist.com/news/business/21677639-business-protecting-against-computer-hacking-booming-cost-immaturity

Traditional central counterparties with a centralised ledger theoretically offer an easy target for cyber attacks as there is a single access point to the system. In contrast, the decentralised nature of the encryption system for each transaction and the impossibility of altering records for a single participant without the consent of the rest should, in theory, make such new systems more resilient to cyber attack.

In 2015, Interpol managed to introduce a proof-of-concept malware programme into a blockchain, showing that it was possible to carry out a cyber attack on a distributed entity. In this case, such an attack would be propagated more easily and faster due to the structure of the register.

IOSCO's "Cyber security in securities markets-An international perspective" published in April 2016 includes a table setting out the main threats to financial market infrastructures in each part of their value chain.

**Examples of cyber security vulnerabilities in financial market infrastructures** TABLE 1

| Stage | Potential threats |
|---|---|
| Pre-trade | Unauthorized access, fraudulent use of a trading participant's algorithm/automated trading systems.<br>Upload of viruses or corrupted files from brokers' systems into trading venues' systems.<br>Dissemination of false information, disruption in access to corporate announcements.<br>Breach in the order management systems resulting in incorrect feeds, false orders or the inability to route orders.<br>Manipulation of index calculation. |
| Execution | Disruption in price discovery in pre-market sessions, trading or periodic call auctions.<br>Manipulation of Financial Information Exchange (FIX) Protocols<br>Interferences with trading venues' matching engines.<br>Disruption in members' connections to trading venue systems. |
| Clearing and settlement | Fraudulent transfer of funds or securities of other clearing members .<br>Manipulation of settlement registers.<br>Undetected access to insider information on open positions and members' and customers' portfolios giving advantages to the attacker.<br>Impossibility of making daily settlements and margin calls. |
| Information dissemination | Shut-down of the relevant information and trade data communications systems. |
| Trade surveillance | Unavailability of surveillance systems.<br>Data corruption of trade records. |

Source: IOSCO and CNMV.

It is essential that securities supervisors can employ, train and continually update the skills of technologically specialist staff so that they can analyse and review cyber security procedures for critical infrastructures within their purview. In the CNMV's case this means the markets and central counterparties included in the Spanish securities market (BME). They are also needed to coordinate work with other national bodies responsible for cyber security of critical infrastructure in each country. In Spain this role is filled by the National Center for the Protection of Critical Infrastructures (CNPIC).

# 4 Directive (EU) 2016/1148 of the European Council and Parliament of 6 June 2016 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive")

The NIS Directive will apply to infrastructure in markets supervised by the CNMV as they are seen as operators of essential services.

Articles 4 and 5 of the directive define an operator of essential services as one whose operations are critical for economic activities. Member states must identify, before November 2018, their operators of essential services and update the list every two years starting in May 2018.

The directive's Annex II includes a list of operators of essential services. Section 4 of the Annex, headed financial market infrastructures, includes trading system operators (regulated markets, MTFs or OTF systems)[15] and central counterparties[16]. Although not mentioned, central depositaries, trade repositories and payment systems should also be seen as essential and critical.

The directive comes into force on 10 May 2018. By then, it will have to be transposed into Spanish law along with implementation of the standards and administrative arrangements needed to ensure its smooth functioning and compliance.

The directive's article 14 lists, among other security requirements, that:

– Market operators will have to take appropriate technical and organisational measures to deal with security risks to their networks and IT systems. These measures must guarantee a level of security appropriate to the potential risks. Specifically, they need to put in place measures to prevent and minimise the impact of incidents affecting networks and information systems of essential services and ensure the continuity of the systems.

Accordingly, member states will be developing coordinated security standards and principles for networks and information systems. The European Commission will publish a list of security principles applicable to market operators.

– Market operators must notify to the competent authority any incidents having a significant impact on the security of the services they provide.

15 Defined in section 24 article 4 of the NIS Directive.

16 Defined in article 2-1 of Regulation EU 648/2012 of the European Council and Parliament.

Competent authorities will have to carry out regular supervision of compliance with incident reporting obligations, with penalties for non-compliance. The authority will also be able to demand that operators provide any information necessary to assess security or carry out security audits.

Member states must put together a computer emergency response team. In Spain this role will be filled by the CNCIP and National Cyber Security Institute referred to in section 3.

The CNMV, particularly its markets department with support from IT systems, must establish contacts with these two entities to assess and supervise the cyber security plans of the financial markets' critical infrastructure firms coming under the CNMV's supervisory scope. At EU level, there will be the European Union Agency for Network and Information Security (ENISA), which includes a unit for critical information infrastructure protection. The unit is charged with supporting competent agencies in each member state, the private sector and the European Commission in the development of a response and recovery plan to threats to critical information infrastructures.

One of this unit's tasks is to develop best practice in areas like the drafting of contingency plans, strategies and minimum cyber security measures, simulations in each country and information pooling.

In July 2014, ENISA set up a working group on information network security in the financial sector. The group aims to:

– Raise awareness of the risks of cyber attack within the financial sector.

– Promote best practice and control throughout entities' organisational structure.

– Develop minimum security measures for information technology infrastructures and specific measures for the banking sector.

Directive 2008/114 on the identification and designation of European critical infrastructures obliges member states to set up a protection system for such infrastructure, which in Spain led to creation of CNPIC.

# 5 Regulations applying in Spain

The CNMV is governed by two sources of cyber security law. First, as part of the general regulations on cyber security, there are two directives, one law and one royal decree, which make specific provisions for operators of essential services.

Second, in the narrower area of international securities market regulation, there is the CPSS-IOSCO guidance, which aims to bolster the resilience of market infrastructures.

The cyber security of Spain's critical infrastructures is a matter of national security and the highest competent national policy body is the CNPIC reporting to the State Secretariat for Security. The secretariat is also empowered to approve the sector strategic plans and designate who counts as a critical operator.

Current measures in force are as follows:

– Law 8/2011[17], of 28 April, on measures to protect critical infrastructure. Critical infrastructure is defined as any strategic infrastructure whose functioning is indispensable and for which there are no alternative solutions, such that their disruption or destruction would have a severe impact on essential services.

– Royal Decree 704/2011[18], of 20 May, implementing the Protection of Critical Infrastructure Regulation.

There are also the National Plan for the Protection of Critical Infrastructure, Strategic Sector Plans, Operator Security Plans, Specific Protection Plans and Operational Support Plans.

## Financial Sector Strategic Plan

Article 20 of RD 704/2011 classifies the strategic sector plans as official secrets overseen by the CNPIC, although they can be seen by ministries, in this case the Ministry for the Economy, Industry and Competitiveness. These plans have to be reviewed every two years.

All departments and bodies that have a copy of the strategic sector plans must comply with the security conditions laid down by the National Security Authority.

Under RD 704/2011, each strategic plan must address at least the following points:

– Risk analysis, vulnerabilities and consequences.

17 https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

18 http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf

– Proposals for organisational and technical measures to prevent, respond to and, if necessary, mitigate possible consequences of the various scenarios considered.

– Proposals for other preventative and maintenance measures (simulations, staff training, communication channels and plans for dealing with adverse scenarios).

– Measures for coordination with the National Plan for the Protection of Critical Infrastructure.

Sector plans are divided into four chapters:[19]

– Chapter 1. Sector regulations.

– Chapter 2. Sector structure.

– Chapter 3. General risk mapping. Includes threat identification, impact scenarios and vulnerability mapping.

– Chapter 4. Proposed strategic measures: organisational and technical, maintenance and coordination with the National Critical Infrastructure Plan.

The sector strategic plans are based on the analysis of a working group which in the case of the financial sector comprised the PIC Commission, the Ministry of the Economy and Competitiveness (General Secretariat of the Treasury and Financial Policy), the Insurance and Pensions Department, Bank of Spain and the CNMV with support from a consultant. Comparing the content of these strategic plans with the IOSCO recommendations, unsurprisingly, reveals much in common.

Designated critical operators, which include regulated markets and central counterparties managed by BME, will have to appoint a head of security and coordination and notify CNPIC to this effect. This person will act as contact point with the competent authorities on cyber security matters. This requirement coincides with the CPSS-IOSCO "Guidance on cyber resilience for financial market infrastructures" summarised in section 6. Specifically, section 2.3.4 of the guidance requires infrastructure firms to appoint a senior manager as responsible for implementing cyber security policy in the organisation.

Critical operators must submit a proposed security plan to the CNPIC for evaluation.

19 According to the article on protection of critical infrastructure: The planning system as a tool of implementation (I). Sánchez Gómez (2014). Security and Citizenship. Ministry of the Interior http://www.interior.gob.es/documents/642317/1203831/Seguridad_y_Ciudadania_N_12_web_126140536.pdf/30e4e817-4105-47e6-8cc0-d32ece569845

# 6 Work on cyber security by the Bank for International Settlements' Committee on Payments and Market Infrastructure

The BIS Committee on Payments and Market Infrastructure (CPMI) set up a working group to assess the significance of cyber security for financial market infrastructures based on the CPSS-IOSCO principles for market infrastructure[20]. These principles break down the various risks confronting market infrastructure firms into legal, market, counterparty, trading and operational risks.

Compliance with the committee's recommendations is already a direct responsibility of the CNMV, particularly with a view to the IMF's future financial sector assessment programmes (FSAP).

The committee's work begins with an initial handicap since none of the principles was originally developed with cyber security risks in mind. As a result, the ability of market infrastructure to prevent and combat cyber attacks is encompassed within the broader principles intended primarily to reduce operational risk, specifically principle 17, which says that *a financial market infrastructure should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls*. To do this, systems should be designed to provide a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim to restore operations with the shortest possible delay, in principle within two hours.

In June 2016, CPSS-IOSCO published its "Guidance on cyber resilience for financial market infrastructures" with the aim of improving resilience. This document does not lay down new principles for infrastructures but rather clarifies and refines the specification of existing principles in the areas of governance (principle 2), risk management framework (principle 3), settlement finality (principle 8), operational risk (principle 17) and links between infrastructures (principle 20). It complements another IOSCO publication from April 2016 "Cyber Security in securities markets-An international perspective" which rounds up the various regulatory measures that IOSCO members had implemented as of that date. Spain was not included among the contributors to the report. The IOSCO guidance describes a five-section cyber security framework for which it lays out a series of practices to strengthen the cyber security of infrastructure operators. The framework will be continuously updated in light of the evolving nature of the threats:

1. **Governance.** This covers all agreements and procedures that an infrastructure has put into practice to manage cyber risks. Measures should not be limited to

20 Committee on Payment and Settlement Systems Technical Committee of the International Organization of Securities Commissions Principles for financial market infrastructures.

technical points but should also include people. Specifically, the firm's management and board will ultimately be responsible for establishing and ensuring compliance with the cyber security plan.

Organisations should foster a corporate culture strongly committed to and aware of cyber security issues. To make sure this happens, the board should include people with the necessary ability and technical knowledge. Corporate culture must be aligned with and committed to cyber resilience and make sure that the whole organisation is engaged with the issue.

Governance includes the abovementioned requirement to appoint a senior manager to oversee implementation and supervision of cyber security policies, with authority, independence and access to the board.

External audits are recommended to periodically assess the infrastructure's cyber resilience.

2. **Identification**. The aim is to identify which of the infrastructure's critical processes and operations need priority protection from cyber attack and allocate resources accordingly. Order management and execution, risk management, supervision and corporate communications systems must be included as critical processes.

   The need to involve the greatest possible number of people from the organisation in cyber security tasks is again emphasised. The report proposes the creation of a committee with representatives from information systems, business lines, legal affairs, HR, communications and risk management. Most of the trading facilities covered discussed in the report have a chief information security officer.

3. **Protection.** Infrastructures must put in place control mechanisms compliant with the most demanding cyber security standards. Such measures may be organisational, such as the creation of operational security centres, or technical, such as anti-virus and anti-penetration systems.

   a. Protection of critical processes and assets. With special emphasis on safeguarding information and identifying weaknesses. It also recommends redesigning processes to incorporate greater segmentation and points of control so that any problems can be isolated.

   b. Links. Implementation of protective measures to mitigate risks and require service providers and participants to provide high cyber security standards.

   c. Internal threats. Detection of anomalous behaviours by staff and controls limiting access to authorised personnel.

   d. Training. With special emphasis and concentration on the group of employees with access to restricted systems and processes.

   The table below summarises the main protective measures and mechanisms put into practice by 34 infrastructure participants in 22 IOSCO member states:

**Examples of protection measures against cyber risks adopted by financial market infrastructures** TABLE 2

| IT management and control | Security controls | Protective technologies |
|---|---|---|
| Compliance with global standards such as ISO, COBIT, SANS Top 20 controls, NIST Cyber security framework and other NIST cyber security standards.<br>Secured software development practices. | Physical security measures.<br>Staff background investigations.<br>Comprehensive password management policy, network access controls.<br>System and data storage segregation.<br>Vulnerabilities testing and protection building before launching new programmes, servers or connections.<br>Security check points. | Web application firewalls (WAFs).<br>Intrusion prevention systems/ advanced persistent threat-detection systems.<br>Defense systems against distributed denial or service (DDoS) attacks.<br>Data loss prevention plan.<br>Antispam filters.<br>Anti-virus and anti-malware systems.<br>Encryption.<br>Port blocking, IP blocking and web filtering.<br>Forensic readiness and incident response tools.<br>Malware analysis. |

Source: IOSCO "Cyber Security in securities markets-An international perspective"

4. **Detection.** Capacity to recognise potential incidents or detect breaches in systems security.

    a. Permanent supervision in real time or with the least possible latency to detect anomalous activities.

    b. Supervision of a wide range of external and internal factors.

    c. Multi-layered controls including of people and processes where each level acts as a security network over previous levels.

5. **Response and recovery.** The capacity of the infrastructure to continue operating, restore critical systems following an attack and reduce systemic risks likely to interrupt activities.

    a. Response plan. To determine the damage and scale of any attack and take containment measures.

    b. Restart in two hours. Critical processes and operations must be restored within two hours of an attack and trades completed and cleared before the next trading session opens.

    c. Contingency plan. If it proves impossible to restart critical operations within two hours there must be an alternative plan covering various scenarios.

    d. Planning and preparation. Infrastructure organisations must prepare and regularly test an attack response and recovery plan.

    e. Links. In the event of attacks compromising data integrity and even the security of back-ups, it is recommended that data should be obtainable from a third party. Market infrastructures are open to their members, who have real-time access to the trading systems and trade repositories.

For this reason, financial firm members can be both a source of contagion and potentially affected by threats.

The report also highlights a number of other practices to improve cyber resilience including simulations, test and cyber intelligence.

This cyber security framework is identical to that proposed by the US Commerce Department's National Institute of Standards and Technology (NIST)[21] and follows many of the standards, guidance and principles set out in the "Framework for Improving Critical Infrastructure Cyber security" published in February 2014.

## Tests and simulations

Testing is a fundamental component of the cyber security framework. All elements of a cyber security programme must be rigorously tested to confirm their effectiveness and identify failures and weaknesses. A testing programme must include:

– Assessment of vulnerabilities and solution of any failures detected.

– Scenario-based tests which assess response, resolution and recovery plans and consider extreme but possible scenarios. Models used should even include hypothetical threats.

– Tests for penetration of systems, networks, processes and staff. These should be run regularly and whenever systems are updated or upgraded.

Regarding the next point, infrastructure organisations should play a part in international industry groups and liaise with sector supervisors with cyber security responsibilities to collect, share and analyse information on cyber security best practice, threats and leading indicators that can help predict possible attacks.

## Cyber intelligence: collection of data on cyber threats

Cyber threats flourish in a constantly changing and evolving environment. In some ways, they are similar to the algorithms used by high-frequency traders which need to be continuously updated to take account of the reactions of competitors.

If they are to do this, infrastructures have to collect and share with other firms and governments information about the cyber attacks they have experienced. The aim is to create a data base of recent and serious threats as well as possible solutions.

Once an attack has been overcome it is useful to disseminate the access routes that it exploited and the solutions proposed to resolve the issue.

– Access to new knowledge and capabilities.

– Predictive capability.

21 https://www.nist.gov/sites/default/files/documents/cyberframework/framework_orientation_20160405.pdf

– Development of metrics to assess the resilience of information systems.

The collection, processing and pooling of information on threats and attacks is one of the points that is consistently highlighted as crucial by all cyber security bodies and experts. Cyber threats are global in nature, often state-sponsored, and the links that allow them to propagate easily across the web make it essential to have an up-to-date data base on attacks and preventative measures. This is what is called cyber threat intelligence sharing. In Spain, the National Cryptological Centre in its paper "*Ciberamenazas 2015/Tendencias 2016*" [22] notes that 90% of the most serious cyber attacks against government and strategic companies have come from foreign governments.

There are various sector initiatives to publicise information on cyber threats, such as http://cyberthreatalliance.org/, http://www.brightcloud.com/, https://exchange.xforce.ibmcloud.com/

Also, in Spain, the CNPIC is working with computer emergency response teams (CERTs) to develop a collaboration, coordination and sharing policy for all information on cyber security threats and incidents as a reaction and response tool to IT security incidents and a way to provide analysis and an early warning system for cyber threats and risks. CNPIC currently has cooperation policies with CERTs including CCN-CERT, CERTSI and INCIBE.

IOSCO's "Cyber Security in securities markets-An international perspective", recognises that although cyber attacks may be dealt with under broader operational risk policies, principle 17 on market infrastructures, they nonetheless pose specific problems that will need to be considered:

– The most sophisticated cyber attacks tend to be persistent and hard to detect and eliminate. These attacks may also be able to propagate themselves silently within a network of IT systems to other infrastructures and/or participating members.

– There may be attacks against which contingency and risk management plans are ineffective, which may corrupt back-up systems so that restoration of the infrastructure's activity could propagate the risk to members.

– There are multiple entry appoints for cyber attacks and as infrastructures are linked to each other and to participants the scope of potential vulnerabilities also includes external actors. Attacks could come via a small-scale member with weak protection measures.

In the international field, IOSCO highlights, in the same 2016 paper, the possibility of centralising all information on attacks and threats. It considers the viability and suitability of IOSCO's Multilateral Memorandum of Understanding (MMoU) as the basis for information sharing among supervisors.

A preliminary version of IOSCO's guidance set out three possible scenarios for infrastructure attacks in ascending order of seriousness.

22 https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015-tendencias-2016-resumen-ejecutivo/file.html

Scenario 1: Breach of confidentiality.

– Theft of the infrastructure's confidential information on assets, positions and customers.

– Such an attack may be the preliminary to a wave of incidents once the security system has been breached.

– It can be hard to detect and resolve.

– It can cause reputational damage to the infrastructure firm.

Scenario 2: Breach of availability.

– Infrastructure services are unavailable.

– Communications between the infrastructure and its members/participants and information providers is compromised.

– The effects of the attack worsen as time goes on.

Scenario 3: Breach of integrity.

– The infrastructure's key data are compromised by the attack.

– It is no longer possible to guarantee the integrity of the systems and information stored in the infrastructure.

– Back-up systems are also affected and their integrity cannot be fully guaranteed.

– Initially the systems seem to be working properly.

– If necessary, a decision must be made to shut down the infrastructure and restart it in an earlier state which can provide the assurance of trade security.

– It may take a long time to detect and analyse the security problem.

– Potential systemic impact as financial instrument positions of market participants could be blocked or not correctly identified.

– It could generate mistrust in financial markets if it cannot be established who owns shares, bonds and other financial instruments.

– Possible contagion to other infrastructures and participants with impacts on liquidity.

One of the key ways to achieve cyber resilience, the report stresses, is to have a defence strategy involving the whole organisation and not just those people directly involved with systems, information and technology. Any workstation connected to the outside world is a potential entry point for cyber threats and it is therefore essential to raise awareness and involve all employees in protective measures. A recent attack on Anthem, one of the biggest US health insurers, broke in through a

phishing attack using email which an employee opened allowing the attackers access to the company's systems[23].

The report proposes measures in three areas: cyber attack prevention, detection and recovery. This will require action on an international scale, including:

1. Harmonising action in different jurisdictions and, specifically, offering support to countries in emerging markets.

2. Promoting and facilitating the sharing of information about cyber attacks recorded in different jurisdictions.

3. Creating a knowledge "library" about cyber security and responses to cyber attacks which is available to authorities and infrastructure operators.

4. Developing the principles to underpin cyber security and resilience as well as a penalty system for criminal conduct.

5. Establishing emergency guidance to be rolled out in the event of large-scale cyber attacks on market infrastructure.

23 http://www.ft.com/intl/cms/s/2/f3cbda3e-a027-11e5-8613-08e211ea5317.html#axzz3uxoWO0PZ