BANCA D'ITALIA
EUROSISTEMA

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Tematiche istituzionali

(Institutional Issues)

Cybersecurity: the contribution of the Bank of Italy and IVASS

Gruppo di coordinamento sulla sicurezza cibernetica (GCSC)

August 2018

BANCA D'ITALIA
EUROSISTEMA

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Tematiche istituzionali

(Institutional Issues)

Cybersecurity:
the contribution of the Bank of Italy and IVASS

Gruppo di coordinamento sulla sicurezza cibernetica (GCSC)

August 2018

This report has been edited by the Gruppo di coordinamento sulla sicurezza cibernetica (GCSC).

Editorial committee

Bank of Italy: Caterina Beccarini *e* Claudia Biancotti *(coordinators),* Alessandro Campi, Antonio Credendino, Riccardo Cristadoro, Sabina Di Giuliomaria, Pasquale Digregorio, Antonino Fazio, Gino Giambelluca, Marilisa Guida, Sonia Guida, Giovanna Partipilo, Adriana Selvaggi*; Ivass:* Sergio Antonica *e* Pietro Franchini.

Editorial assistants for the Italian version: Fabrizio Martello *e* Rosanna Visca *(Bank of Italy).*

The English edition is translated from the Italian by the Language Services Division of the Secretariat to the Governing Board and Communications Directorate

Address
Via Nazionale 91 – 00184 Rome – Italy

Telephone
+39 0647921

Website
http://www.bancaditalia.it

ISSN 2283-3226 (print)
ISSN 2283-3250 (online)

Designed and printed by the Printing and Publishing Division of the Bank of Italy

CONTENTS

Foreword

Cyber attacks are a growing threat to an economy that is increasingly based on digital technologies. Cyber risk is relevant to numerous production and consumption activities and, by its very nature, it crosses national and sectoral borders.

Thus, a global and systemic approach is called for. In an interconnected world, no digital device – however well protected – can be considered as totally secure if the surrounding environment is still vulnerable. Cooperation between public authorities and the private sector is of central importance and society as a whole – not only the experts – must be made aware of the risks involved.

Principles, best practices, rules and technological standards are being set to strengthen the prevention, defence and reaction capabilities of countries, organizations and businesses. These initiatives are flanked by national cybersecurity strategies. Italy is also moving in this direction.

The Bank of Italy and IVASS are in the front line of the battle against this threat as they are the institutions responsible for keeping the Italian financial system secure, especially given that it is a prime target for hostile actors, be they motivated simply by profit or by a desire to trigger a crisis of confidence. Repelling attacks is essential to safeguarding savings and ensuring that the economy runs smoothly.

The Bank of Italy and IVASS have established the *Cybersecurity Coordination Group* (GCSC), which brings together a set of specialists with expertise in: ICT, the supervision of banks, financial intermediaries and insurers, payment system oversight and economic research. The aim is to develop strategic thinking on cyber risk and to ensure a line of action that can be used for all these different functions.

This report provides an overview of what has been accomplished to protect the financial sector from cyber attacks.

The Senior Deputy Governor

Salvatore Rossi

Introduction and summary

Overview

Information and Communication Technologies – or ICT – are expanding rapidly, thanks to the productivity gains they make possible. In fact, a growing number of sectors that are vital to the economy and finance are completely dependent on them. The value of 'Big Data' – extremely large data sets from which artificial intelligence draws complex information – is increasing. The number and types of objects connected to the internet is also expanding, for example industrial machinery, domestic appliances, cars, video cameras, and lighting systems, to create what is known as the Internet of Things (IoT).

Nevertheless, there are new risks alongside the new technologies, the most important of which is cyber risk, linked to actions that exploit the vulnerabilities of an ICT device or of its underlying code with the aim of making it stop working, obtaining unauthorized access to the data it holds, or compromising it in some way.

Until a few years ago, cyber risk was limited to a few specific areas, such as defence, because advanced technologies were mostly concentrated in large data processing centres and also because cyber attacks were very costly to carry out. With the expansion of access to computer networks and the deployment of cheaper tools for such attacks, cyber intrusion is not only motivated by political or military reasons, but is now also driven by profit (see Section 1).

The amplification of the cyber threat means that governments are facing complex policy challenges. Malicious software and other forms of cyber attack can cause significant damage to state security and the economy, in the same way as conventional weapons. National legal systems and international law are adapting to the new scenario.

Unauthorized access to computer systems became a criminal offence in several countries in the 1990s. Since the early 2000s, the main advanced and emerging economies have developed broader strategies to provide the institutional architecture for crisis prevention and management, measures to enhance the security of the public sector and critical infrastructures, incentives to train specialists and set up public-private partnerships, as well as certification schemes for software and hardware security (see Section 2.1).

Initiatives in the area of international cooperation, which are essential to address a global threat, are still weak. Within the context of cooperation between countries that share key strategic safety objectives, such as NATO and the G7, there has been progress only on specific issues such as coordination between police forces in the fight against certain crimes (see Section 2.1). The financial system is partly an exception in that regulatory cooperation on a wider basis is favoured by the existing experience on other fronts – especially in relation to financial stability – and by the global dimension of some key players.

The techniques used to conduct cyber attacks are evolving rapidly. Receiving updates on the vulnerabilities of computer systems and how these are being exploited by hostile outsiders enables us to implement a proactive defence, which is much more effective than a reactive one. Timely sharing of information is therefore fundamental for defence. However, not everyone who has suffered an attack or identified weaknesses is willing to share what they came to know, so it is necessary to guarantee confidentiality and reciprocity. In some cases, these conditions are created spontaneously within groups of economic operators that are particularly sensitive to cyber risks. Increasingly, the public authority takes on the role of catalyst and confidence builder.

There have been two more successful information-sharing models: the first is based on the information and analysis centres (ISACs), and the second on computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs; see Section 2.1).

National and European regulation

The Italian regulatory framework mirrors the European Union's cybersecurity strategy, of which Directive (EU) 2016/1148 on the security of network and information systems (NIS) constitutes the backbone. The Directive provides that EU Member States shall require operators of essential services for the economy to adopt appropriate security measures; it also provides for the establishment of a Cooperation Group within the EU for the exchange of information and best practices (see Section 2.2 and the box 'The NIS Directive in Italy' in the same chapter).

For various parties, ICT security requirements are also derived from two other recent European provisions: Regulation (EU) 2016/679 – the GDPR (see the box 'The General Data Protection Regulation (GDPR)' in Chapter 2) and Directive (EU) 2015/2366 – the PSD2 (see the box 'The Revised Payment Services Directive (PSD2)' in Chapter 3). Further obligations could arise from the approval of the 'Cybersecurity Act' presented in 2017 by the European Commission, which confers on the Union the power to certify the security of the devices and related software.

Italian cybersecurity regulation is currently based on two measures:

a) Prime Ministerial Decree of 17 February 2017 ('Gentiloni Decree'), which confers on the Government's Security Intelligence Department (DIS) the responsibility for coordinating the prevention and management of cyber crises through the Cybersecurity Unit (Nucleo per la sicurezza cibernetica, NSC) composed, on a permanent basis, of representatives from the ministries sitting on the Interministerial Committee for the Security of the Republic (CISR), i.e. Defence, Interior, Foreign Affairs, Economy and Finance, Economic Development, and Justice (see Section 2.3);

b) Legislative Decree 65/2018, which implements the Directive on security of network and information systems (NIS), establishes the national computer security incident response team (CSIRT), makes the Security Intelligence Department (DIS) the point of contact with the EU institutions and identifies the authorities

responsible for the implementation of the measures provided for in the Directive as regards strategic economic sectors.

Cybersecurity in the financial sector

The financial system is a prime objective for cyber attacks and, because of the numerous interdependencies, damage caused by such attacks can be massive and have systemic effects.

Central banks and other supervisory authorities play a crucial role in ensuring the cybersecurity of the financial system. In many countries, they manage vital components, such as payment systems; they may require supervised entities to provide information on attacks; order the adoption of appropriate safeguards; and sanction those that do not comply (see Section 3.1).

In the financial sector, the main forum for international cooperation in the field of financial market infrastructures and payment systems is the Committee on Payments and Market Infrastructures (CPMI) of the Bank for International Settlements (BIS). In relation to supervision, the most significant bodies are: the Senior Supervisors Group (SSG), the Financial Stability Board (FSB), and the BIS's Basel Committee for Banking Supervision (BCBS). The most important reference document is 'Guidance on cyber resilience for financial market infrastructures' (in this report, the 'Guidance'), published in 2016 by the CPMI, together with the Board of the International Organisation of Securities Commissions (IOSCO; see Section 3.2).

A central role is also played by the G7 Cyber Expert Group (G7-CEG), which is currently in the process of establishing an international cooperation protocol for use by authorities to respond to cross-border incidents.

Within the Eurosystem, the European Systemic Risk Board (ESRB) ensures a high-level connection for financial stability purposes between the European Commission, authorities in the sector,[1] the Eurosystem and national macroprudential authorities. As regards banking supervision, the EBA has issued guidelines on ICT risk monitoring of banks by the competent authorities (see Section 3.3).

Within the Eurosystem, the ECB, in cooperation with the national central banks, ensures the security of the TARGET2 and TARGET2-Securities platforms. It also establishes cyber regulations for payment systems and market infrastructures operated by third parties. The Single Supervisory Mechanism (SSM) verifies compliance with security requirements by the banks, collects reports of major cyber incidents, and coordinates management procedures in the event of a crisis.

In 2017, the ECB Governing Council approved the supervision strategy for cyber resilience in relation to European market infrastructures. This strategy includes the establishment of a public-private collaboration forum, the European Cyber Resilience Board (ECRB), set up in 2018 (see Section 3.3).

---

[1] European Banking Authority (EBA), European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA).

In addition to the traditional regulatory and supervisory tools, the Eurosystem is developing a framework for the technical testing of system security which will be completed by the end of this year for payment and market infrastructures.

The role of the Bank of Italy and of IVASS

The Bank of Italy carries out various tasks to strengthen both its cybersecurity (in that it runs critical infrastructure, provides digital services and is the custodian of sensitive data) and the financial system as a whole, as the supervisory authority for payment systems and other market infrastructures, as well as being the authority for banking and financial supervision (see Chapter 4).

Similarly, IVASS, as the supervisor of the insurance system, carries out various activities to monitor and strengthen its digital security (see Chapter 5).

The Bank of Italy and IVASS are:

– establishing appropriate internal safeguards, which include the Bank's Computer Emergency Response Team (CERTBI);

– participating in international and European technical meetings of central banks and the financial sector;

– issuing national regulations to strengthen the governance of processes and safeguards in the field of cybersecurity;

– regulating and supervising market infrastructures and national financial operators;

– collecting data on cyber vulnerabilities and incidents;

– exchanging data and research with other institutions dealing with defence against cyber attacks;

– stimulating a public-private collaboration in sharing data and creating defence capabilities, including through the operation of an Italian financial sector CERT (CERTFin) together with the Italian Banking Association (ABI);

– raising awareness among young people and adults about the use of digital financial services by means of financial education campaigns;

– collecting and analysing statistical data on the frequency and economic impact of cyber attacks on the Italian private sector;

– assessing cyber risk in relation to insurance products such as specific cyber insurance policies and their distribution.

In order to better coordinate all the activities taking place in different organizations and units, the Bank of Italy and IVASS established the '*Cybersecurity Coordination Group*' (GCSC) in 2017.

1. Context factors

Cybersecurity, seen in the past as merely a technical issue that is linked to the business continuity of specific processes, today impacts more and more skills and domains. The expansion of the sectors involved and the knowledge required is a consequence of the digital transformation of the economy and the dependence on numerous digital services; many everyday tasks now take place in 'cyberspace'.[2] Going forward, the growth of the Internet of Things, i.e. the set of devices connected so as to engage in the real world, will open up both domestic and production activities to the cyber dimension, in a qualitatively different manner than is currently the case.

The devices, as well as the software and the network connections which make up the cyberspace have technological and organizational vulnerabilities that can be exploited maliciously, as can be seen by the proliferation of cyber attacks.[3] An unsafe cyberspace is a major weakness in a digitalized society, not only as a result of damage that attacks can cause directly on target structures, but also because a widespread perception of insecurity may undermine the functioning of markets that are vital for the economy, and which are based on the availability, integrity and confidentiality of digital data. In the medium term, cyber attacks could also slow the take-up of new technologies, with a negative impact on productivity and growth.[4]

The cyber threat, which is pervasive, anonymous, polymorphic, transnational, and asymmetric,[5] requires a system-wide response, partly because weaknesses in some areas of cyberspace lead to problems in others (negative externalities).[6] This principle is expressed both in the *National Strategic Framework for Cybersecurity* adopted by the Italian Government (in Italian only; see Section 2.3) and in equivalent documents published by the main OECD countries. A number of public and private actors must work together to ensure the overall security of the cyberspace.

Not only those working in this field but also society as a whole must be made aware of the risks. Many cyber incidents are actually the result of imprudent behaviour, such as the use of overly simple passwords. It is not enough to invest in anti-virus software and other technical defences: a real paradigm shift is needed, including in cultural and organizational aspects.[7]

---

2 Cyberspace is defined as 'all interconnected ICT infrastructure, including hardware, software, data and users, as well as the logical relationships between them. It includes, among other things, the internet, communication networks, system actuators and mobile equipment with a network connection', see Presidenza del Consiglio dei Ministri (2013a).

3 For a review of the major computer incidents made public in the past decade, see CSIS (2018).

4 See, among others, World Economic Forum (2014) and CSIS (2018).

5 A. Fazio and A. Leotta (2015), p.71.

6 T. Moore and R. Anderson (2012).

7 Benoît Cœuré, Member of the Executive Board of the ECB spoke of a paradigm shift, pointing out that 'we have to accept that cyber attacks are inevitable and that attackers are persistent. Consequently, we have to establish how – in the case of persistent attacks – we prioritize our operations and resources, protect our key assets and restore functionalities. Cyber resilience goes beyond technology, it also encompasses governance, company culture and business processes' (B. Cœuré, 2017). This paradigm shift is also mentioned in A. Fazio and F. Zuffranieri (2018).

Cyber risk is not new: in the early stages of the digitization process, however, both potential victims and attackers were limited in number. Only a few sectors, such as defence and telecommunications, were sufficiently computerized as to be vulnerable to cyber attacks. What is more, the knowledge and resources required to prepare and unleash such attacks existed almost exclusively in the military context or in that of some research centres. Over the years, computer use and access to electronic networks have greatly expanded, multiplying the number of targets; in addition, the skills needed to develop malicious codes (malware) are now at the disposal of many criminal organizations, which develop tools to carry out attacks and sometimes sell them at very low cost to a wide range of customers. While politico-military attacks still play a pivotal role, there has been a large number of attacks carried out by individuals driven by potential profit.

Given its central role in the production system, the financial sector is a primary target both for those seeking financial gain and for those who want to jeopardise the orderly functioning of the economy. There is a vast area exposed to attack because of the intensive use of ICT by the financial industry, which has been one of the fastest to exploit the new digital tools. This is even more so today, since, as a result of the development of Fintech, hi-tech financial services are now mostly delivered online.

An example of a critical target is the SWIFT network. This connects more than 11,000 parties in 200 countries: its messaging system is used by banks, market infrastructure managers and public authorities in their financial intermediation activities. There have been numerous attacks on this network in recent years, in some cases even involving central banks.[8]

---

[8] In 2016, the unauthorized use of SWIFT messages by a criminal group led to the theft of about USD 80 million from the Central Bank of Bangladesh. A private bank in Taiwan was attacked in the same way in 2017, with a loss of around USD 60 million (most of which was later recovered). A similar episode, but on a much smaller scale, recently involved the Russian central bank.

2. The institutional and regulatory framework

2.1 National cybersecurity strategies and international cooperation

The escalation of cyber threats has meant that states have been facing complex policy challenges; cyber attacks have the potential to harm the rights of citizens and states, in the same way as conventional weapons.

In a number of countries criminal law has been updated since the 1990s introducing offences such as unauthorized access to computer systems. Since the early 2000s, the advanced economies and key emerging countries have developed broader approaches to enhancing cybersecurity as part of their national security strategy.

Such strategies are at different stages of development but share common elements:

– completion of the institutional architecture for crisis prevention and management;

– measures to enhance the security of the public sector and critical infrastructures;

– incentives for public-private cooperation and training for specialists;

– software and hardware security certification schemes.

Sharing information on attacks and threats is of particular importance for national strategies. As intrusion techniques are evolving rapidly, keeping up to date on the vulnerabilities of computer systems and the ways criminals exploit them marks the line between effective and ineffective defence. However, enterprises that have suffered attacks are reluctant to disclose information on them for fear of reputational spill-over effects; they are willing to share data only in situations which guarantee confidentiality and reciprocity. Sometimes groups of economic operators that are particularly sensitive to cyber risks (e.g. critical infrastructure managers) pool their knowledge voluntarily; more often, intervention is required by the public sector, which acts as a guarantor and helps to create and maintain a climate of confidence.

There are two very successful information-sharing models. The first relies on information and analysis centres (ISACs) which allows a stakeholder group to pool information and analytical capabilities. The second is based on Computer Networks Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs),[9] established inside government bodies, companies and trade and industry associations[10] which link up to share information, analysis capabilities and

---

[9] In theory, a CERT has a more general mandate than a CSIRT: the former intervenes in any emergency that puts the functioning of an ICT system at risk (including, for example, those caused by breakdowns or natural events), while the latter is activated only in the case of security breaches. In practice, the two acronyms are often used to refer to the same activities; in this report they are considered as equivalent.

[10] Each CERT/CSIRT carries out activities in favour of a specific reference community known as a 'constituency'. It can be defined in terms of users or of protected technology.

operational defence capabilities (see the box 'The origins and development of the CERT/CSIRT networks').[11]

The origins and development of the CERT/CSIRT networks

The military defence departments of the main advanced countries had organizational structures dedicated to ICT security as far back as the 1980s. In some cases they also cooperated with the academic world to analyse the evolution of the threat and to develop defences, especially in the United States. Some hi-tech firms were already allocating resources to cyber protection long before the term came into common use.

At that time, there was still no widespread awareness of the fact that a cyber attack could hit several targets simultaneously: any intrusions were mainly isolated incidents (in 1986, for example, some West German hackers recruited by the Soviet intelligence service, the KGB, had stolen secrets from American defence networks). It was not thought particularly necessary for victims to work together to analyse and prevent attacks.

This outlook changed in 1988, when computer science student Robert Morris (currently a lecturer at the Massachusetts Institute of Technology) wanted to measure the size of the internet. He created some software which exploited a vulnerability in the UNIX operating system to replicate automatically on all the terminals connected to the internet at any given moment, and which would send data on each one back to Morris. Although this software was not designed to interfere with the activity of the computers involved, it contained a programming error which actually made the terminals unusable. According to the International Telecommunications Union, a United Nations agency, Morris's software blocked about 10 per cent of the 6,000 computers connected to the internet at that time.

Researchers at the Defense Advanced Research Projects Agency (DARPA), the American military body that created the internet, discovered that the victims of the 'Morris worm' had mainly dealt with the problem individually: each of them had used resources to identify the problem, work out how to solve it and repair the damaged systems. A cooperative approach, based on sharing information and defence tools, would have saved a great deal of time and money.

The US government then decided to set up the Computer Emergency Response Team Coordination Center at the Software Engineering Institute at Carnegie Mellon University in Pittsburgh: this was the first time that the acronym CERT was used officially. The coordination of US CERTs is now in the hands of federal bodies, although at Carnegie Mellon University there is still a CERT, which is regarded as a benchmark for excellence.

---

[11] The main international networks of CERT are:(a) the Forum of Incident Response and Security Teams (FIRST), established in the United States – an international confederation of CERTs, set up in 1990, which brings together over 300 organizations of different countries and sectors; (b) the Trusted Introducer Network, established in 2000 by the community of European CERTs, which numbers more than 100 organizations.

While national and regional initiatives (for example, at European level) have generally produced good results, those involving international cooperation – essential to address a global threat – are still weak. There has been progress only on specific issues, such as coordination between police forces in the prevention of certain crimes, and in the context of cooperation between countries sharing key strategic security objectives, such as NATO and the G7.

The UN General Assembly has not yet succeeded in reaching consensus on the application of international law to conflicts arising in the cyberspace. In particular, there are still differences between countries as to the conditions under which a state-sponsored cyber attack can be considered as an act of war and might thus legitimise self-defence on the part of the state under attack (pursuant to Article 51 of the Statute of the United Nations)[12] or trigger multilateral military intervention (Article 42).[13]

2.2 The European Union's Cybersecurity Strategy

EU cybersecurity legislation was first drafted in the early 2000s and, at the time, focused on combatting crime. At that stage, the provisions on network security, which were not limited to police aspects, only applied to the telecommunications sector. In the following years, the need to ensure the overall security of information was highlighted as key to pursuing the objectives of promoting the values of freedom and democracy. In 2008, with Council Directive 2008/114/EC on critical infrastructure, basic protection measures were introduced, including in respect of technological threats for European critical infrastructures.

In 2013, a joint communication was drawn up on the EU's cybersecurity strategy.[14] As far as civil defence is concerned, the cornerstone of this strategy is Directive (EU) 2016/1148 on the security of network and information systems (the NIS Directive), which was issued in 2016 with a requirement for Member States to transpose it into national law by May 2018. The European legislator has provided for Member States to designate a national authority to impose strict security requirements on operators of essential services for the economy (energy, transport, banking and finance, health, drinking water supplies, and telecommunications) and digital service providers (online search engines, online marketplaces and cloud computing services). The Directive has introduced a requirement for these operators to notify the authorities of incidents that

---

12 'Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security'.

13 'Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations'.

14 It identifies five priorities: enhancing cyber resilience, i.e. the ability to repel cyber attacks and recover quickly if hit; drastically reducing cybercrime; developing a cyber defence policy and the corresponding capabilities under the Common Security and Defence Policy; developing the industrial and technological resources for cybersecurity; and establishing an international policy regarding actions carried out by states in the cyberspace.

may have a 'significant impact' on service continuity. The definition of the criteria for identifying the significance of such incidents is left to the Member States.

The Directive also established an EU cooperation group for the exchange of information and good policy practices. The Group aims to strengthen crisis response capacities by introducing an obligation for each country to have a public CSIRT, which, in the event of a cross-border incident, must cooperate with the equivalent teams established in other Member States.

A further EU measure called the General Data Protection Regulation (GDPR) came into force in 2018 for the protection of individuals in relation to the processing of personal data. The new rules, which apply to both public and private entities, require that those holding and processing personal data maintain higher security standards than in the past (see the box 'The General Data Protection Regulation – GDPR').

The General Data Protection Regulation – GDPR

EU Regulation 2016/679 (GDPR) came into force on 25 May 2018; it applies to the processing of personal data in EU Member States and marks the shift from a formal to a substantive concept of data protection. The new rules are based on the principle of data protection by default and by design: personal data processing must be designed primarily to safeguard the right to confidentiality of the interested parties. To this end, both technical measures – including those pertaining to cybersecurity – and organizational models must be adopted to minimize the likelihood of wrongful access to information.

A great deal of weight is attached to the accountability of personal data controllers, for example, employers holding employees' personal data or service providers that keep customers' personal data, who must comply with the principles established by the GDPR. Controllers are obliged to notify the supervisory authority of any data breaches; they must also inform the interested parties should there be any risk to their rights or freedoms. This innovation is particularly significant as it exposes a very broad group of people to the risk of legal action, namely all personal data controllers and processors, which could stimulate an overall strengthening of cybersecurity and growth in the insurance market.

The GDPR is underpinned by a strong sanctions regime. Financial penalties can be as high as €20 million for the most serious cases or four per cent of turnover, whichever is higher.

Some sectoral measures complete the framework (for those related to the financial system, such as the Directive on payment services in the internal market, see Section 3.3 and the box 'The PSD2 Directive' in Chapter 3).

In 2017, the European Commission presented its proposal for an EU 'Cybersecurity Act'. If approved, it would lead to the introduction of a single form of cybersecurity certification in the EU for hardware and software, which would potentially have a very

significant impact by applying to the digital sphere the stringent standards that are already applied in regard to the physical safety of goods produced in the EU. The EU Cybersecurity Agency (ENISA) would be responsible for certifications[15] and its role would be greatly increased, while until now it has been limited to carry out operational and technical tasks (such as organizing exercises), studies and advisory services for the Member States.

2.3 Italy's Cybersecurity strategy

In Italy, as in the European Union, the first cybersecurity initiatives focused on combatting crime. In the 1990s, offences were introduced into the Criminal Code and the task of addressing them was entrusted to the Postal and Communications Police.[16]

In the early 2000s, public authorities were required to improve their cybersecurity levels.[17] Shortly afterwards, the intelligence service's expertise in cybersecurity was strengthened, in particular with regard to protecting information that is confidential or considered to be a state secret.[18] In 2008, the national critical information infrastructures were identified[19] and the National Cybercrime Centre for Critical Infrastructure Protection (CNAIPIC) was established. Subsequently the first formal procedures were introduced for managing cyber events in relation to national security. A comprehensive approach to the matter took root between 2012 and 2014. In 2013, two documents were published by the Prime Minister's Office: (a) the National Strategic Framework for Cybersecurity, with the aim of identifying tools and procedures for enhancing the country's cyber capabilities; (b) the National Plan for Cybersecurity, which transforms the Strategic Framework's forecasts into operational guidelines. A national CERT was also set up for citizens and businesses, within the Ministry of Economic Development,[20] and a CERT for public authorities within the then newly-created AGID (Agenzia per l'Italia digitale).[21] In addition, the information gathering capacity in the field of cybersecurity was enhanced by security intelligence agencies.[22]

The Prime Ministerial Decree of 17 February 2017 (the 'Gentiloni decree') rationalized the institutional architecture of cybersecurity, bringing all responsibilities within the remit of the Prime Minister's Office (Figure 1).

---

15 Through its high-level collaboration in the network for information security within the EU, ENISA has been operating from its headquarters in Greece since 2004 as a centre of expertise for cybersecurity in order to develop culture and knowledge of this field for the proper functioning of the internal market. The Agency cooperates closely with the Member States and the private sector in three different areas: recommendations, activities to support the development and implementation of policies and practical activities in direct collaboration with operational teams, such as the Computer Security Incident Response Teams (CSIRTs).

16 Laws 547/1993 and 269/1998.

17 Prime Ministerial Directive 16 January 2002.

18 Decree Law 144/2005, converted into Law 155/2005.

19 Interior Ministry Decree of 9 January 2008 implementing Decree Law 144/2005.

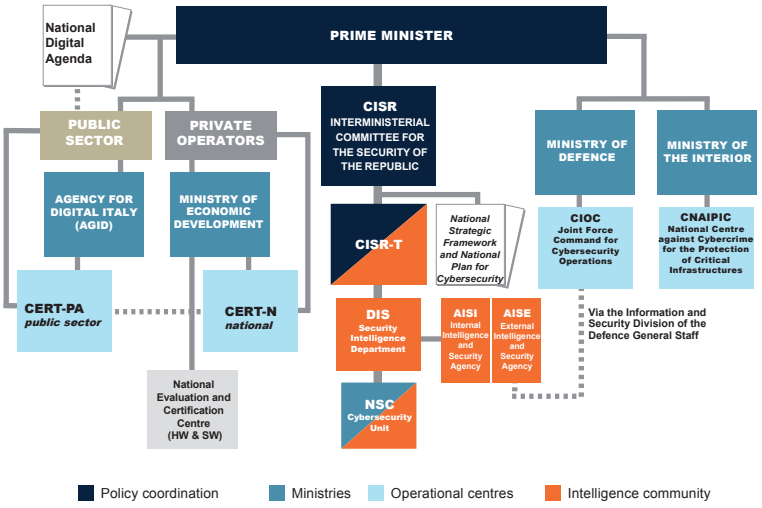
20 Legislative Decree 70/2012.

21 Decree Law of 22 June 2012, converted with amendments into Law 134/2012.

22 Law 133/2012.

Figure 1

NATIONAL CYBERSECURITY ARCHITECTURE AS DESIGNED BY THE GENTILONI DECREE

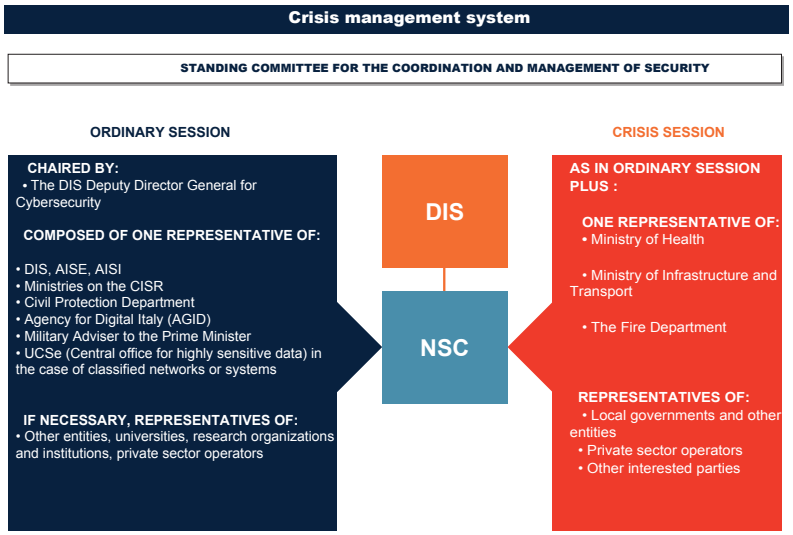


Source: Based on data provided by the Prime Minister's Office (2018).

The Prime Minister's office issues its policy guidelines through the Interministerial Committee for the Security of the Republic (CISR), in which various ministries take part (Defence, Interior, Foreign Affairs, Economy and Finance, Economic Development and Justice). Operational activities are coordinated by the Security Intelligence Department (DIS) within the Prime Minister's Office, which also heads the Cybersecurity Unit (NSC), which is in charge of crisis management (Figure 2).

Figure 2

CRISIS MANAGEMENT SYSTEM UNDER THE GENTILONI DECREE



Source: Based on data provided by the Prime Minister's Office (2018).

The Gentiloni Decree was followed by the publication in March 2017 of the second edition of the National Plan for Cybersecurity, updating the operational risk prevention tools and underlining, among other things, the need to improve public-private coordination.

In May 2018, with the transposition into law of the NIS Directive, further action was outlined to strengthen the country's defences and an Italian CSIRT was set up at the Prime Minister's Office, bringing together the national and the public sector's CERTs (see the box 'The NIS Directive in Italy'). On the regulatory side, the Italian Parliament empowered the Government to adapt Italian legislation on measures for the security of personal data (see the box 'The General Data Protection Regulation – GDPR').

The NIS Directive in Italy

Legislative Decree 65/2018, implementing Directive (EU) 2016/1148, on the security of network and information systems (NIS), lays down a multi-faceted system of responsibilities. Consistently with the architecture designed by the Prime Ministerial Decree of 17 February 2017 (the 'Gentiloni Decree'), the Prime Minister's Office is at the top of the pyramid and is in charge of setting policy and coordinating the tasks envisaged by EU legislation: (a) formulating the national cybersecurity strategy, (b) coordinating with the European Union and other Member States through the Government's Security Intelligence Department (DIS) and (c) the centralized collection of information on incidents and monitoring of threats through the Italian Computer Security Incident Response Team (CSIRT).

The Decree also identifies the competent authorities for each sector, which are tasked with identifying the operators of essential services, laying down minimum security measures, monitoring their implementation including by means of inspections, and imposing penalties. The relevant authorities are:

– The Ministry of Economic Development covers the energy sector, digital infrastructure and services;[1]

– The Ministry of Infrastructures and Transport is responsible for the transport sector;

– The Ministry of Economy and Finance, in cooperation with the Bank of Italy and Consob (the Italian companies and stock exchange commission), covers the banking sector and financial markets infrastructure;[2]

---

1 The telecommunications sector is excluded from the scope of application of the NIS Directive because it is covered by specific regulations. The definition of operators of essential services under the NIS Directive instead includes providers of internet exchange points (IXP), domain name system (DNS) services (i.e. the infrastructure that makes it possible to reroute network traffic by transforming a network address in the uniform resource locator format, or URL, for example www.bancaditalia.it, into the IP address of the destination server) and top level domain (TLD) services, i.e. the infrastructure used to manage the assigning of domain extensions such as '.it' or '.com' for internet websites.

2 Does not include payment and settlement systems; the Directive does not affect the regime under Union law for the Eurosystem's oversight of these systems (see Recital 14 of the Directive and the ECB Opinion of 25 July 2014).

– The Ministry of Health and, as applicable, the Regional Governments and the Autonomous Provinces of Trento and Bolzano, are responsible for healthcare;

– The Ministry of the Environment and, as applicable, the Regional Governments and the Autonomous Provinces of Trento and Bolzano, for the provision and distribution of drinking water.

As far as the public sector is concerned, AGID issued minimum ICT security measures for public administrations, comprising an orderly and logical set of controls, i.e. precise technical and organizational actions aimed at preventing the risk of cyber attacks and mitigating their negative effects.[23] The Three-Year Plan 2017-2019 for ICT has been adopted, defining the reference model for the development of information technology for the public sector and the operational strategy for the digital transformation of the country. The Plan provides for the rationalization of ICT resources as the preferred method to increase the level of security by reducing exposure to cyber attacks.

[23] AGID Circular 2/2017.

3. Cybersecurity within the financial system and the role of the sectoral authorities

3.1 Attacks on the financial system

The financial system is the prime target for threat actors, who are encouraged by the potential financial gains or want to disrupt the orderly functioning of the economic system for political reasons. As early as 2014, a coordinated attack on numerous US banks led, among other things, to the theft of the personal data of 80 million customers of JP Morgan Chase. Many more attacks of this kind were carried out in the following years. Almost none of the large private financial institutions has been immune and some central banks have also been affected.[24]

Attacks on the financial system sometimes use very simple methods, such as the theft of credentials to access accounts via phishing, or by overloading servers with millions of simultaneous requests for data, thus rendering network banking services inoperable and resulting in a 'denial of service'. Sometimes the intrusions are carried out using complex methods leading to the removal of funds or data on a large scale.

Defending the financial system is a complex task: the sector is highly digitalized; it is globally interconnected via a small number of infrastructures that may have vulnerabilities and can be undermined by imprudent behaviour on the part of any of hundreds of millions users of online financial services. A successful attack can be extremely harmful even if carried out on a small scale: some central processes in the financial system are crucial, such as timely data for the payment settlement system where even modest delays can lead to high costs.

Outside the framework of defence and national security, sectoral authorities were among the first to pay attention to cyber risk, understanding the potential negative impact, not only on operators who have been personally affected, but also on public confidence in the financial system. Malware has been developed that is capable of spreading very rapidly, causing genuine epidemics, thus making the systemic risk of highly connected financial processes and systems even greater (see the box 'Two global cyber attacks: WannaCry and NotPetya').

Two global cyber attacks: WannaCry and NotPetya

In the early months of 2017, a group of hackers known as the Shadow Brokers spread a ransomware worm on the internet that was used by criminal groups to create tools to make highly virulent attacks.

This code replicates itself very quickly using new and sophisticated stratagems created to make infecting computers extremely easy.

---

[24] See Footnote 8.

This mechanism was the basis for two of the biggest cyber crises in recent years. In May 2017, hundreds of thousands of Microsoft Windows users were hit by WannaCry, a program that blocks a computer by encrypting its data and demands a ransom in Bitcoin for decrypting them. Some British hospitals had to postpone medical appointments and surgical procedures because their computer systems were down.

In June 2017, another attack was carried out by spreading NotPetya software, which is even more dangerous because it encrypts data permanently, thereby destroying the contents of the computers it attacks. The Danish multinational company Møller-Mærsk declared damages of about $300 million; other industrial groups said they had suffered serious consequences, though without specifying the exact sums.[1] According to newspaper reports, the global impact of NotPetya came to over one billion dollars.

These two attacks exploited the known vulnerabilities of the most common platforms. The number of victims was high but limited by the fact that many firms had updated their systems in good time.

---

[1] C. Biancotti and R. Cristadoro (2018)

Even where central banks are not responsible for regulating and supervising financial intermediaries, in most countries they are of prime importance in driving the process of strengthening the financial system. They often directly manage or have oversight responsibilities for vital infrastructures, such as payment systems.

Cyber risk also concerns the insurance sector, with companies that are widely exposed because they form part of the value chain and are connected to other parts of the financial system (banks and conglomerates).[25] The typical operational aspects of any life, damage or health insurance, which involve many online interactions with the insured, expose operators to the legal risks related to the theft of confidential information.

On the other hand, safeguarding against cyber risk is a market opportunity for the insurance sector, with the development and supply of products to prevent the adverse effects of cyber attacks (see Section 5.3). This is still an immature market at global level;[26] however, it is developing fast and the sectoral authorities have a central role to play in ensuring that the nature of cyber risk, with its high correlation between events and the significance of major incidents, does not pose a solvency threat to insurance companies.

---

[25] These companies are of varying sizes with very different levels of organizational safeguards (agencies, brokers, and individual agents).

[26] OECD estimates show that in the US, where more than 80 per cent of the global market is concentrated, between 20 and 35 per cent of firms have specific coverage. The percentage in the UK, which is the second largest market in the world, and continental Europe is even lower; see OECD (2017).

3.2 International responses

In the financial sector, international cybersecurity cooperation has achieved good results, including in broader contexts, at least as regards defining guidelines and best practice. This has been facilitated by previous experiences on other fronts, the most important being that of financial stability, and the global dimension of some of the key players.

In contrast to political developments, central banks, market oversight authorities and banking and financial intermediaries have reached consensus on some key documents, including countries with very different policy agendas: the most important example is the 'Guidance on cyber resilience for financial market infrastructures', published in 2016 by CPMI-IOSCO.[27] In line with international supervisory principles,[28] the Guidance suggests methods and tools to ensure the business continuity of market infrastructures in the case of cyber attacks. Even though it is addressed to a specific category of operators, it has become a reference publication for the entire financial system.

Other broad-based cooperation initiatives are those launched by the FSB as mandated by the G20. The main ones are:

– the preparation of the Cyber Lexicon – a glossary for the financial sector in the area of cybersecurity and resilience. It aims to remove any terminological ambiguities and support consistent international initiatives by reducing the differences between national regulations which often aggravate the compliance burden of supervised entities;

– scenario analyses conducted by the Standing Committee on Assessment of Vulnerabilities (SCAV) to assess the potential systemic impact of cyber attacks;

– the inclusion of cyber risk in the early warning exercise carried out together with the International Monetary Fund.

In 2016 the International Association of Insurance Supervisors (IAIS) produced a fact-finding document on the evolution of cyber risks, mitigation practices and the approaches adopted by the authorities.[29] The OECD, according to which the dissemination of cyber risk insurance policies is key to enhancing the security of the economy, has issued recommendations to insurance companies and supervisory authorities.[30]

Nevertheless, no global consensus on technical guidelines and standards has yet been reached on issues more closely related to national security, such as information-sharing, coordination between countries in responding to cyber crises that have cross-border effects and the methodologies for testing the defences of private financial operators (see the box 'Intelligence-led "red team" testing: characteristics and problems').

---

27 The Basel Committee on Banking Supervision was also involved in an advisory role.

28 CPSS-IOSCO (2012).

29 IAIS (2016).

30 OECD (2017).

Only within the G7 has any progress been made – the Cyber Expert Group (G7-CEG) set out the high-level non-binding principles for the testing of information systems and, as regards international communication and cooperation between financial authorities, it is developing a protocol to be followed in the event of a cross-border crisis.[31] This protocol will be tested in 2019 in a simulation exercise. The G7-CEG also established a forum for discussion with the private sector to identify information exchange strategies and appropriate regulatory actions.

Intelligence-led 'red team' testing: characteristics and problems

In order to assess a firm's cyber defences, checking whether it complies with regulatory requirements is not enough; it is also advisable to simulate attacks as realistically as possible. One of the models considered most effective for this purpose involves testing carried out by an intelligence-led team of pseudo-attackers (called a 'red team', an expression borrowed from military exercises). To measure the quality of a target firm's defences, a group of investigators called 'threat intelligence providers' are first asked to assess how hostile subjects could exploit the firm's organizational, procedural and technological vulnerabilities and to describe them in a Targeted Threat Intelligence Report. Based on this report, a second independent group – the red team – plans and carries out specific simulation exercises to assess the defences of the potential target.

Since the red team may find vulnerabilities in the target firm or come across classified information, if these exercises are carried out by unreliable persons and without appropriate guarantees, they may in turn become a source of further risk. These aspects are even more significant in the financial sector; with the support of the private sector, some governments and financial authorities have introduced reference frameworks for controlled simulation exercises that envisage certification and accreditation schemes for threat intelligence and red team service providers.

3.3 The European context: recent developments

The highly globalized financial system means that, at least in advanced countries, regional initiatives are generally in line with international ones. This is particularly true for market and payment infrastructures. The cybersecurity guidance issued by the CPMI-Iosco (see Section 3.2) is the main frame of reference adopted by the European System of Central Banks (ESCB) and the Eurosystem. This is also the case in the area of banking supervision, where the current ideas regarding cyber risk within the EU and the Eurosystem are the same as those held internationally. However, important regional and national differences remain because banking systems are closely linked to their local economic and institutional contexts.

The European Systemic Risk Board (ESRB) ensures a high-level connection for financial stability purposes between the European Commission, European supervisory

[31] G7-CEG (2016) and (2017).

authorities (EBA, ESMA, EIOPA), the Eurosystem and the national macroprudential authorities. Within the ESRB, the ESCG (European Systemic Cyber Group) analyses the potential systemic impacts of cyber attacks with particular reference to the European economy.

3.3.1 Market and payment infrastructures

In March 2017, following a proposal from the Market Infrastructures and Payments Committee (MIPC), the Governing Council of the ECB approved the oversight strategy for cyber resilience for European market infrastructures, which had been developed by a task force comprising representatives of 14 central banks and other European authorities with the aim of ensuring in the Eurosystem a common application consistent with the CPMI-IOSCO Guidance.

The strategy, which will be fully implemented by 2019, identifies three objectives: the strengthening of individual market infrastructures, with specific reference to payment systems; the strengthening of the sector as a whole; and the promotion of public-private cooperation at European level.

To achieve these objectives, the MIPC has developed:

a) a questionnaire and an analysis model to collect and evaluate information on the compliance of European market infrastructures with the provisions of the abovementioned Guidance on cybersecurity;

b) a framework for the advanced testing of ICT systems (European threat intelligence-based ethical red teaming; Tiber-EU);[32]

c) a set of oversight expectations, which are a self-assessment tool for the regulated entities and a basis for interaction between the regulated entities and the authorities.

The European Cyber Resilience Board (ECRB) was also set up in 2018 as a strategic discussion forum to facilitate and support public-private cooperation on the cyber resilience of the European financial system.[33]

3.3.2 Supervision of banking and financial intermediaries

In the European context, the guiding principles for banking supervision in the field of cybersecurity are set out by the EBA, which defines the security requirements for supervised entities and the harmonized supervisory rules for Member State authorities. To this end, it has issued guidelines for payment services, as required by the updated version of the EU Directive on payment services (see the box 'The PSD2 Directive').

---

[32] The 'Tiber-EU Framework' was approved by the Governing Council of the ECB and published in May 2018. To supplement the framework, the 'Services Procurement Guidelines' was published in August 2018.

[33] The ECRB is chaired by the ECB and composed of payment and other market infrastructure operators, critical service providers and European-wide payment circuits. Members are identified and designated by the ECB for a period of two years. The ECRB is composed of seven central banks with permanent membership and three central banks with rotating membership. In addition, the following are invited to participate as observers: ESMA, ENISA, EUROPOL, EBA, ECB/SSM and the European Commission.

In 2017, the EBA also published recommendations on the outsourcing of cloud computing services in the financial sector and guidelines for supervisors on ICT risk assessment, including cyber attacks. These tools allow for the standardisation and integration of supervisory practices in EU countries.

The PSD2 Directive

Directive (EU) 2015/2366 on payment services in the internal market (PSD2), which replaces the previous Directive (EU) 2007/64, entered into force in the Member States in January 2018 and contains the regulations for managing the security of payment service providers. The latter are obliged to adopt risk mitigation measures in their internal management and in their interactions with customers (e.g. strong customer authentication) and with other payment service providers (e.g. secure communications with new Fintech operators authorized to access bank accounts).

The Directive also introduces an obligation to report major security incidents (Article 95), to be identified according to the European Banking Authority's guidelines. The notification must be addressed to the competent authority of the Member State where the payment service provider is based; the authority then provides the EBA, the European Central Bank and any other national authorities that might be interested with the details of the event (Article 96). Introducing notification obligations has two objectives: (a) to prevent events that by their nature could trigger a 'domino effect' in the financial system and (b) to improve the capacity to respond rapidly to such events at a systemic level.

In 2017, the EBA introduced some important innovations and published some regulatory technical standards on ICT security for payment service providers such as banks, post offices, electronic money institutions and other payment institutions.

For Europe, a central role is played by the Single Supervisory Mechanism (SSM) which, since 2015, has been equipped with a framework for cooperation between the ECB and the national authorities in order to ensure the shared, effective and efficient management of any cyber attacks against significant banks. A database of incidents has been established, with input via mandatory reporting by banks. The operational management of crises is entrusted to a dedicated task force.

Based on specific risk indicators arising from incident reports or by weaknesses found in offsite controls, the SSM launches cyber risk inspections.

3.3.3 The insurance sector

In the insurance sector, the process of regulatory and supervisory harmonisation is coordinated by EIOPA. As regards governance, the Solvency II regulatory framework provides that insurance undertakings ensure their business continuity, also by developing continuity plans that deal with ICT risks.

EIOPA is also monitoring the provision of cyber risk insurance policies across Europe.

3.4 The Italian legislative framework

The European rules for this sector, as described above, also apply to Italy's financial system. In addition to this legislation, the national measures issued by the Bank of Italy, IVASS and Consob apply.

With the entry into force of the NIS Directive, the cyber protection of credit institutions and other relevant market infrastructures is incorporated in the broader national framework (see Section 2.3 and the box 'The NIS Directive in Italy') with the establishment, among others, of a formal partnership between sectoral and governmental authorities.

4. The role of the Bank of Italy

4.1 Cybersecurity and the Bank of Italy

The Bank of Italy has long encouraged the digitalization of the financial system, with special emphasis on ICT security. In the past, this function mainly involved safeguards against operational risks and strategies to ensure business continuity. It is precisely in this context that awareness of the cyber threat initially emerged.

The Bank chairs the *Comitato per la continuità di servizio della piazza finanziaria italiana* (Codise), a business continuity unit set up in 2003 to coordinate crisis management in the Italian financial marketplace. Systemic financial sector operators and Consob participate in the Committee.[34] Codise regularly carries out crisis simulations as an exercise; these included, as early as 2008, the possibility of cyber attacks.

With the evolution of technology and the proliferation of attacks, in addition to business continuity, other areas have gained importance. The Bank of Italy is currently carrying out a number of activities to strengthen the security of its internal IT (see Section 4.2) and that of the financial system (see Section 4.3). It also conducts research on the cybersecurity of the economy as a whole, as vulnerabilities in other sectors could also affect the security of the financial system (see Section 4.4).

The Strategic Plan 2017-2019 highlights the importance of cyber risk in two of its action plans: the first is to 'enhance the Bank's cybersecurity in relation to new risk scenarios' as part of the strategic objective of being more innovative and efficient; the second is to 'promote innovation and resilience in the Italian financial sector' as part of the objective to promote innovative, efficient and secure payment services in Italy and Europe.

To respond to the cyber threat, all the different profiles (technical, operational, regulatory, oversight, supervision and economic) have to be considered together. In 2017, in order to better coordinate the activities carried out in different national and international working groups, the Bank of Italy and IVASS established the Cybersecurity Coordination Group (GCSC).

4.2 The Bank of Italy as a critical infrastructure

The Bank of Italy must maintain a very high level of internal ICT security because:

– it is identified as a national critical information infrastructure as defined in the Ministry of the Interior's Decree of 9 January 2008 (see Section 2.3).

34 Codise cooperates with governmental authorities and other public and private institutions involved in crisis management and business continuity for national critical infrastructures. Through Codise, the Bank participates in crisis communication and management exercises at the European and international levels (e.g. the ECB's TITUS exercise). Since 2014, the role of Codise is explicitly referred to in the banking and financial supervision rules and in the guidelines for market infrastructure business continuity.

In this capacity, it cooperates with the National Centre for Critical Infrastructure Protection (CNAIPIC), which is part of the Postal and Communications Police Service;

– it provides digital services to the Eurosystem (for example, via the TARGET2 and TARGET2-Securities platforms) and services to national government bodies such as the State Treasury, government debt auctions, and the General Government Transactions Information System (SIOPE);

– it is the owner of personal data in electronic form under the terms of the GDPR.

The Bank's digital defence safeguards have recently been strengthened through:

– the development of the Bank's cyber resilience strategy based on sectoral and international guidelines and best practices;

– the creation of (a) the Bank's own Computer Emergency Response Team (CERTBI), (b) a Security Operations Centre (SOC), and (c) a Network Operations Centre (NOC);

– the planning of a cyber defence programme requiring investment in digital resources, including to update and improve dynamic defence measures;

– the introduction of organizational and technical innovations for the Bank to comply with the new European privacy rules (see the box 'The General Data Protection Regulation – GDPR' in Section 2).

The Bank is contributing to the drafting of a joint proposal for supplying security services for the ESCB.

4.3 Cybersecurity of the financial system

The Bank is responsible for cybersecurity in the financial system:

– as the oversight authority for the payment system and supervisor of the other market infrastructures; within the Eurosystem, it shares this responsibility with the ECB and the other national central banks. The aim is to increase the cyber resilience of financial market infrastructures. The Bank has taken part in drafting the main international guidelines (see Section 3.2) and is involved in the development of the Eurosystem's strategy (see Section 3.3). In the framework of the cooperative oversight of SWIFT, the Bank of Italy is collaborating in the monitoring of the Customer Security Programme (SWIFT-CSP) which consists of a series of requirements and security controls required of users following the recent cyber attacks conducted on a global scale;

– in its capacity as the national supervisor of the banking and financial system, it has introduced specific requirements for the management of banks' information systems with the revision of Bank of Italy Circular No 285/2013 (Supervisory Rules for Banks). These requirements include ICT security measures for supervised entities, as well as the obligation to report major security incidents, including cyber attacks. Within the SSM, the Bank of Italy participates in the cyber risk assessment of significant banks, which began in 2015 when a self-assessment questionnaire was sent out to banks in order to identify those that were most exposed, so that they could be the subject

of more detailed on- and off-site supervision. In addition, in the European context, the Bank participates in the drafting of the EBA's ICT and security risk guidelines for banking and financial intermediaries. At international level, within the Senior Supervisory Group and the Basel Committee on Banking Supervision, it is working on the definition of best practices for cybersecurity.

In 2017, the work of CERTFin (the Computer Emergency Response Team for the Italian financial sector) began, sponsored by the Bank of Italy in close cooperation with the Italian Banking Association (ABI) to support the sharing of information about cyber threats and the improvement of techniques for responding to cyber attacks experienced by the banks. CERTFin is an example of a successful public-private partnership, also acknowledged by the Italian Security Intelligence Department (DIS) in its annual report to Parliament (*Relazione sulla politica dell'informazione per la sicurezza*). The largest players in the national financial system (banks and market infrastructures) joined in on a voluntary basis, as did numerous smaller participants. In 2017, CERTFin analysed and shared with its members about 1,000 alerts as to possible attacks, security breaches, and technological vulnerabilities, two thirds of which involved threats, including malware dissemination campaigns and attempted fraud.

Given the importance of prudent behaviour on the part of users of online financial services to counter the cyber threat, the Bank is also committed, through its financial education initiatives, to raising the awareness of young people and adults as regards digital financial services.

Table 1 shows how financial sector protection activities, including those in which the Bank of Italy is directly involved, form part of the broader national and international contexts.

Table 1

PROTECTION OF THE FINANCIAL SYSTEM AT THE VARIOUS LEVELS

Level	Policies	Financial sector
INTERNATIONAL Rules for behaviour in the cyberspace; resiliency for strategic sectors; cooperation	– G7/G20 Leaders' Declarations; – UN Group of Governmental §Experts' reports (up to 2015)	– G7-CEG: high level non-binding principles (Fundamental elements); – G20/FSB: census of supervisory rules and practices; Cyber Lexicon; – CPMI-IOSCO Cyber Guidance; – IAIS and OECD inspections of the insurance sector
EUROPEAN Secure and accessible cyberspace for the development of the European digital economy	– EU Cybersecurity Strategy (2013); – Proposal for EU Cybersecurity Act (2017); – NIS Directive; – GDPR Regulation	– Market infrastructure: Eurosystem cyber resilience strategy; – Payment service providers: PSD2 Directive; EBA guidelines; – SSM supervision of significant banks; targeted inspections for cyber risk; – Solvency II requirements regarding business continuity for insurance companies
NATIONAL Protection of the economy against cyber threats	– Prime Ministerial Decree of 17 February 2017; – Legislative Decree 65/2018 – National Strategic Framework for Cyberspace Security; National Plan for Cyberspace Protection and ICT Security	– CERTBI; CERTFin (Bank of Italy/ABI); – Bank of Italy/IVASS regulation/supervision in areas of national competence, including the implementation of the Directive on the security of networks and information systems (NIS); – The Bank of Italy's Strategic Plan 2017-19

4.4 Cybersecurity of the economy as a whole

The Bank of Italy also provides a contribution in terms of statistical data collection and economic research. In a digitalized economy, the cyberspace security is a key factor in a country's development and competitiveness. The relevant literature shows that the market does not ensure optimal levels of protection due to externalities and information asymmetries.[35] Policy measures are therefore needed, which in turn require two essential elements: credible data and an adequate understanding of microeconomic dynamics in the ICT security market.

There are still some significant shortcomings here. While growing rapidly, the theoretical literature is still at the early stages and, as regards the empirical literature, there is a still a scarcity of high-quality data on the frequency and cost of attacks. Most statistics quoted by the media are produced by commercial companies selling defence systems. However valuable these data may be, above all in indicating the emergence of new threats, they are not completely reliable because of a potential conflict of interest.

The Bank of Italy carried out a survey, the first of its kind in Italy, on the frequency and economic impact of cyber attacks on the private non-financial sector,[36] The first results, which concerned the frequency and distribution of attacks by area, sector and size class, were published in February 2017. Six months later, estimates of companies' expenditure on protecting against cyber attacks and of the damage and costs associated with such attacks were released.[37] These data are essential both to guide the economic analysis and to define appropriate public intervention mechanisms (see also Chapter 16 'Cyber risk in the Italian economy' in the Bank of Italy's *Annual Report for 2017*, 2018).

---

35 See, for example, R. Anderson (2001) and C. Biancotti et al. (2017).

36 At present, similar data from official sources are only available for the United Kingdom. The data were collected via the Cyber Security Breaches Survey, conducted for the first time in 2016.

37 C. Biancotti (2017a) and (2017b).

5. The role of IVASS

5.1 IVASS and cybersecurity

ICT and cyber risk is also relevant to Italy's Insurance Supervisory Authority (IVASS) in terms of:

a) the continuity and security of its own institutional functions and processes (an aspect that also involves the confidentiality of information);

b) the cybersecurity of insurance companies;

c) the impact of the development of the cyber risk insurance policy sector on the stability of the insurance system.

As regards (a), IVASS's activities mainly use the platforms, systems and services provided by the Bank of Italy on the basis of the technological integration between the two institutions, set out in the law establishing IVASS and in the 2014 Framework Agreement. This has enabled IVASS to meet the requirements for continuity and cybersecurity (as regards its infrastructure, procedures, services, workstations and personal computing devices) in a similar way to the Bank of Italy.

Cybersecurity and cyber risk issues are dealt with following the procedures of Operational Risk Management (ORM), which include an assessment of existing risks and of possible ways of managing vulnerabilities. Staff training focused on improving the knowledge of cybersecurity issues, including governance and security processes.

5.2 Cybersecurity and insurance companies

Since 2014, IVASS has been monitoring the state of cyber risk exposure in the insurance sector, including by means of a questionnaire as part of its quarterly surveys of firms' vulnerabilities and risks.[38] It has also investigated the security of agents and brokers.

Based on its survey of insurance undertakings, in 2017 IVASS sent the insurance market a letter containing measures and recommendations for enhancing cybersecurity, and announced it would be carrying out a new survey in 2019.

---

[38] The largest insurance companies indicated that they had started mitigation processes for business continuity and for risk management and control in proportion to the nature, scale and complexity of their business. Business impact analyses help in identifying critical circumstances to be detected in advance and managed with specific contingency plans. The largest companies also reported the implementation of cyber risk prevention, monitoring and management programs, supported by cyber governance – which in some cases involves establishing specific committees or functions such as the Chief Information Security Officer – and the application of security standards. Cooperation in managing cyber risk implies membership of cybersecurity organizations at various levels (including government bodies) and the exchange of information with the Postal Police and with business associations, so that economic losses deriving from technological risks can also be tracked.

In line with the regulatory developments and the insurance sector's operational environment, IVASS is working on the revision of the reference legislation for companies and financial intermediaries. In July 2018, the new rules on corporate governance for companies and insurance groups were issued, including safeguards against cyber risk under these rules.

In conjunction with EIOPA, further steps have been taken to:

– enhance the resilience of the insurance sector, as regards both business continuity and cyber risk, including through information campaigns;[39]

– promote the implementation of sector-wide activities by insurance companies, including through public-private partnerships, to be coordinated with initiatives already undertaken in the banking and financial sector.

5.3 How the dissemination of cyber risk insurance policies may impact the stability of the insurance sector

IVASS has launched initiatives to monitor the exposure of the Italian insurance industry to cyber risk and the market for insurance policies to cover this risk. As regards such insurance policies, some initiatives were carried out in cooperation with the Bank of Italy. The monitoring of market developments is also carried out as part of IVASS's activities in relation to new insurance products.

As regards the dissemination of insurance policies, the Italian market has shown similar trends to the rest of Europe. The marketing of specialized products, which was approached very cautiously in the past, shows signs of growth, with more companies involved, although volumes are still very small.[40] According to data published by ANIA in 2017, only 5 per cent of Italian firms take out specific cyber risk insurance;[41] Bank of Italy surveys of industrial and non-financial service firms show just how small this market is for firms. A recent survey carried out by IVASS, with the participation of five major insurance groups, also confirms – from the supply side – the limited size of the market for cyber risk insurance policies in Italy.[42]

---

39 *InsurTECH: digital innovation in the insurance market* (2017).

40 Products not only include coverage for cyber risk and the associated costs related to civil and criminal proceedings, but also provide protection against identity theft and civil liability for damages resulting from the violation of the privacy legislation. The development of the market is hampered by certain limitations, which can be attributed to the complexity of this type of risk and its reliance on technical evaluations which are constantly evolving, both on the supply side (limited penetration, difficulty in the proper pricing of the risk, lack of historical data and of reinsurance coverage) as well as on the demand side (a combination of lack of awareness and high moral hazard, difficulties linked with adapting the distribution network, business skills, and support infrastructures).

41 C. Savino, *Cyber risk, Insurance and SMEs*, Milan, 7 March 2017.

42 There are three types of insurance contracts: (a) *Retail customers* (approximately 2,000 contracts with an average insured amount of EUR 300 and a maximum of EUR 150,000); (b) *Small businesses* (approximately 5,000 contracts with an average insured amount of EUR 30,000 and a maximum of EUR 250,000); and (c) *Large corporates* (less than 50 contracts with an average insured amount of between EUR 3 million and EUR 20 million, and a maximum of EUR 50 million).

More up to date and detailed information will be available in EIOPA's analysis of the European insurance market currently under way, including a thematic review of the use of big data as well as the dissemination of technological innovation and of the risks it poses.

References

AGID (2017), *Piano triennale per l'informatica nella Pubblica amministrazione. 2017-2019*.

Anderson, R. (2001), *Why information security is hard. An economic perspective*, in *17th Annual Computer Security Applications Conference*, conference proceedings, New Orleans, LA, 10-14 dicembre 2001, Los Alamitos, CA, IEEE Computer Society, 358-365.

BCE (2018), *Tiber-EU Framework. How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*.

Biancotti, C. (2017a), *Cyber attacks: preliminary evidence from the Bank of Italy's business surveys*, Banca d'Italia, Questioni di economia e finanza (Occasional papers), No. 373.

Biancotti, C. (2017b), *The price of cyber (in)security: evidence from the Italian private sector*, Banca d'Italia, Questioni di economia e finanza (Occasional papers), No. 407.

Biancotti, C. and R. Cristadoro (2018), *The machine stops: the price of cyber (in)security*, in "VoxEU.org", 17 January 2018.

Biancotti, C., R. Cristadoro, S. Di Giuliomaria, A. Fazio and G. Partipilo (2017), *Cyber attacks: an economic policy challenge*, in "VoxEU.org", 23 June 2017.

CSIS (2018), *Significant cyber incidents*.

Cœuré, B. (2017), *Introductory remarks*, address given at the *High-level meeting on cyber resilience*, Frankfurt am Main, 19 June 2017.

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

CPSS-Iosco (2012), *Principles for financial market infrastructures*.

Department for Digital, Culture, Media & Sport [UK Government], Ipsos MORI and University of Portsmouth (2018), *Cyber security breaches survey 2018*.

Fazio, A. and A. Leotta (2015), *Attacchi informatici e* cyber-security, in *La continuità di servizio dei sistemi informatici. Il data centre incontra gli utenti*, conference proceedings, Banca d'Italia, Rome, 22 April 2015, 71-88.

Fazio, A. and F. Zuffranieri (2018), *Interbank payment system architecture from a cyber security perspective*, Banca d'Italia, Questioni di economia e finanza (Occasional papers), 418.

G7-CEG (2016), *G7 fundamental elements of cybersecurity for the financial sector*.

G7-CEG (2017), *G7 fundamental elements for effective assessment of cybersecurity in the financial sector*.

IAIS (2016), *Issues paper on cyber risk to the insurance sector*.

InsurTECH: l'innovazione tecnologica nel mercato assicurativo (2017), conference proceedings, Ivass, Rome, 15 December 2017.

Moore, T. and R. Anderson (2012), *Internet security*, in Peitz, M. and J. Waldfogel (edited by), *The Oxford handbook of the digital economy*, Oxford, Oxford University Press, 572-599.

OCSE (2017), *Enhancing the role of insurance in cyber risk management*.

Presidenza del Consiglio dei ministri (2013a), *Il linguaggio degli organismi informativi. Glossario intelligence*, in "Gnosis. Rivista italiana di intelligence".

Presidenza del Consiglio dei ministri (2013b), *Piano nazionale per la protezione cibernetica e la sicurezza informatica*.

Presidenza del Consiglio dei ministri (2013c), *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*.

Presidenza del Consiglio dei ministri (2017), *Piano nazionale per la protezione cibernetica e la sicurezza informatica*.

Presidenza del Consiglio dei ministri (2018), *Relazione sulla politica dell'informazione per la sicurezza 2017*.

World Economic Forum (2014), *Risk and responsibility in a hyperconnected world*.

All links valid as of August 2018