16. CYBER-RISK AND THE ITALIAN ECONOMY

Digital and ICT technologies play an increasingly important role in the world economy. In 2016, some 95 per cent of firms in the OECD countries used the Internet and 77 per cent had a website. More than half of the adult population made at least one purchase online during the course of the year; in 2010, the figure was 36 per cent.[1]

The use of ICT is growing in Italy as well, although overall it is still below the OECD average. According to Bank of Italy data, in 2017 one fifth of Italian firms with 20 or more employees in industry and non-financial private services also sold their products online; 13 per cent had industrial machinery, CCTV, lighting systems, sensor networks and other equipment that could be connected to the Internet (Internet of things, IoT), while 7 per cent collected and analysed big data. Approximately one third of Italian consumers bought a product or service online.[2]

Almost all production processes and a growing number of consumer activities take place at least in part in cyber-space. This includes, for example, the physical infrastructure of the Internet and other computer networks, the set of IT protocols and programs for communicating within these networks, the information that is exchanged, and 'smart' production equipment and consumer goods (smartphones, smart TVs and so on).[3]

Even a firm or person that is not directly using advanced technologies nevertheless relies on services – financial, logistic and data transmission – that do.

The new technologies bring evident advantages: they increase business productivity and allow consumers a wider choice of goods and services at lower prices. They can also be a factor in economic and social inclusion: in some low-income economies, the advent of mobile banking has enabled access to the financial system even in remote areas far from any large urban centres, where in any case few bank branches exist.

Alongside these benefits, digitalization brings costs and risks for the economy. Some of these have been the subject of study and reflection on the part of economists because they replicate, albeit in different forms, the problems raised by innovation in the past. These include the unemployment of workers whose skills have been rendered obsolete by the new technologies, the growing wage disparity between workers with different levels of qualification, and the emergence of dominant positions in some markets thanks to network externalities. By contrast, the risk of

[1] OECD, *Digital Economy Outlook*, 2017.

[2] Istat, *Cittadini, imprese e ICT*, 2017.

[3] Presidenza del Consiglio dei Ministri, *Glossario intelligence*, 2013.

cyber-attacks, which can also have significant systemic consequences, has been less studied by the economic profession.

The economic impact of cyber-risk

Cyber-risk is not new: in the early stages of digitalization, however, the number of both potential victims and perpetrators was small. Only a few sectors, such as defence and telecommunications, were sufficiently computerized to make them vulnerable to attack. Moreover, the know-how and resources required to plan and carry out such attacks were available almost exclusively to the military and some research centres. Over the years, as the use of IT equipment and access to the Internet has expanded dramatically, the number of potential targets has multiplied. Meanwhile, the skills required to program and distribute malware have become available to numerous criminal organizations that develop malicious tools and even market them online at low cost to a broad customer base.

In 2017 the damage caused by two computer viruses, WannaCry and NotPetya, cost businesses and public institutions hundreds of millions of dollars, including the UK's National Health Service, the Danish shipping giant Moller-Maersk and the multinational pharmaceutical corporation Reckitt Benckiser. From 2016 to 2017, cyber-attacks against financial institutions linked to the interbank payments system via the SWIFT network wiped out huge sums of money and even affected some central banks.

Cyber-risk should not take second place to any of the other problems that have arisen with digitalization. Cyber-attacks can cause significant financial damage to the targets and create a perception of insecurity, which in turn can undermine the operation of those markets that are based on the availability and circulation of digital data and are by now vital to the global economy.

Guaranteeing the cyber-security of firms, networks and infrastructure is not just a technological problem. Their vulnerability often stems from an undervaluation of the risks and from distorted incentives that lead to organizational failings, imprudent behaviour of staff, and insufficient investment in protection. Many attacks are carried out using simple tools that could easily be neutralized.

Software and hardware manufacturers have a very strong incentive to enter as early as possible a market in which, because of significant network externalities, a product's success depends on the number of users that choose it (as, for example, is the case of messaging platforms and operating systems). The adoption of higher standards of security is therefore sacrificed in the interests of rapid distribution. Moreover, hackers often do not attack their target directly, particularly if it is a large, well-protected business; instead, they seek out weaker third parties with access to the target's network and prey on their vulnerability. In either case, lack of attention to cyber-security produces negative externalities: in practice, those who market products that are not secure and those who do not protect their systems properly are not the ones that bear the cost of a cyber-attack.

Sales contracts for software and hardware usually exclude civil liability for damage to clients caused by cyber-attacks. In the case of the third parties whose vulnerability is

exploited in the course of an attack, there is in general no automatic means by which the actual victim can obtain compensation without going through a judicial process of uncertain outcome.

One of the main obstacles to correcting these distortions and setting up systems to defend against cyber-attacks is the lack of information about their occurrence and their impact. The cyber-security data gap was highlighted by the G7 Finance Ministers and Central Bank Governors, and under Italy's presidency[4] they have encouraged countries and institutions to find suitable solutions.

Measuring the frequency and cost of cyber-attacks in Italy

Since 2016 the Bank of Italy has collected data on the cyber-risk affecting Italy's production system. It analyses firms' investment in cyber-security, the frequency and financial impact of cyber-attacks as well as the use of specialized insurance policies. This is the first database in Italy – and one of the few worldwide – that complies with standards of statistical representativeness, transparency of method and publication of micro-data.

Many of the difficulties encountered in collecting the data and estimating the relevant aggregates, such as the frequency of cyber-attacks on a given range of potential targets and the calculation of their direct and indirect financial cost, can be overcome, at least in part, by using suitable statistical methods (see the box 'Measuring the economic impact of cyber-attacks').

MEASURING THE ECONOMIC IMPACT OF CYBER-ATTACKS

Obtaining reliable estimates of the frequency and costs of cyber-attacks presents significant methodological difficulties. The data are generally collected by interviewing a sample of firms that do not always have the technical ability to identify past breaches or are reluctant to report them for fear of reputational repercussions.[1] The impact of cyber-attacks is therefore potentially underestimated.

In the Bank of Italy's analyses[2] the sample data acquired in the Survey of Industrial and Service Firms are corrected to take account of these eventualities. Firms that declare they do not monitor their IT systems (in all likelihood including those that potentially failed to detect an attack) and firms that skip the questions on cyber security despite having completed the rest of the questionnaire (potentially reticent firms), are assigned responses in line with those provided by comparable firms in terms of size, sector of activity, or other characteristics. Observing the sample, there is a higher probability that small, low-tech firms fail to detect an attack

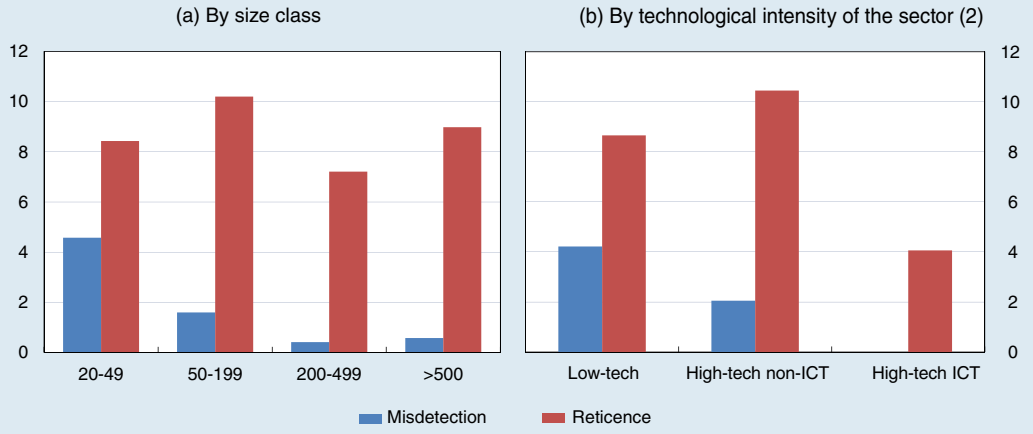
[1] E. Gal-Or and A. Ghose, 'The economic incentives for sharing security information', Information Systems Research, 16, 2, 2005, 186-208.

[2] C. Biancotti, 'Cyber attacks: preliminary evidence from the Bank of Italy's business surveys', Banca d'Italia, Questioni di Economia e Finanza (Occasional Papers), 373, 2017.

[4] G7, *Communiqué*, issued on the occasion of the meeting of Finance Ministers and Central Bank Governors, Bari, 12-13 May 2017.

(with a correspondingly greater correction), while reluctance to report a breach is more widespread among high-tech firms that do not belong to the ICT sector, with no significant differences based on size (see the figure).

Correction model for underestimation of attacks in 2017 (1)
(firms to which an attack is imputed; per cent)



Source: Survey of Industrial and Service Firms, 2017.
(1) Share of firms – in each size class or by degree of technological intensity – whose responses were corrected (by assigning at least one breach to them) based on the statistical model. – (2) According to the OECD/Eurostat classification that distinguishes between, in manufacturing, firms with high and low technology intensity and, in services, firms with high or low knowledge intensity, assimilated here to comparable manufacturing firms; firms operating in the ICT sector are isolated within each high-tech category. Firms in the energy sector, not covered by the original classification, are reclassified as non-ICT high-technology.

In addition to the failure to detect attacks and firms' reluctance to report them, impact assessments are further hindered by how difficult interviewees find it to quantify some costs (such as lost earnings due to a business outage or a loss of competitiveness)[3] and by the fact that the statistical samples used in the surveys, constructed to be representative of the main economic trends, do not permit accurate estimations of low-probability events such as major cyber-attacks.[4] Combined, these factors suggest that the overall costs are probably underestimated.

Even if these difficulties were resolved, we would still not have a satisfactory assessment of what cyber-attacks cost the entire economy, i.e. one that incorporates both the direct impact on the companies affected and that on third parties. For example, if computerized network infrastructures in the financial, energy or telecommunications sectors slow down, there are costs not only for managers but also for users. Their estimation is de facto hindered by the lack of in-depth knowledge of digital interdependencies and value chains in the economy; estimates should be based on a sample of incidents rather than on firms and, for each incident, account should be taken of the economic impact on all parties.

[3] O. Livingston, M. Shabat and T. Cheesebrough, 'Cost of cyber incidents', acts of the 16th Annual Workshop on the Economics of Information Security, San Diego, 2017.

[4] UK Department for Culture, Media and Sport, *Cyber security breaches survey: main report*, 2017; C. Biancotti, 'The price of cyber (in)security: evidence from the Italian private sector', Banca d'Italia, Questioni di Economia e Finanza (Occasional Papers), 407, 2017.

More reliable data will be available in the coming years as recent international, European and national laws require a wide range of companies to notify the authorities of successful breaches. For attacks that compromise the confidentiality of personal information, the onus to report it may also be on citizens whose data have been violated. The new EU General Data Protection Regulation[5] is particularly incisive in this respect and since 25 May 2018 has introduced in Europe the same obligations that already apply in the US.

Combining administrative archives based on these reports with data from the sample surveys would mark a crucial step forward in enriching our knowledge of existing interconnections and enabling the total cost to the economy of cyber-attacks to be estimated more accurately.

[5] Regulation (EU) 2016/679 with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The data reveal that Italy's production system is extremely heterogeneous as regards the management and awareness of cyber-risk (Table 16.1). The median expenditure on cyber-defence per firm is around €4,530, which is about 15 per cent of the gross yearly salary of a non-managerial employee. And there are significant differences between sectors: for low-tech firms the figure often barely reaches €3,500, while it is higher among large firms; in the ICT sector it tops €19,000.

Table 16.1

Cyber-security expenditure, cyber-defence awareness and frequency of cyber-attacks
(per cent of firms unless otherwise indicated)

FIRMS	Median expenditure (1)	Employee training	Vulnerability analysis	Data encryption	Attacks (raw data) (2)	Attacks (adjusted data)
			Sector (3)			
Low-tech	3,420	60.4	51.9	29.1	13.6	26.2
High-tech non-ICT	6,930	74.2	66.1	36.1	17.0	29.3
High-tech ICT	19,080	95.0	91.6	77.1	19.8	23.9
			Size class			
20-49	3,120	59.5	50.8	28.6	13.6	26.4
50-199	7,770	73.7	66.1	37.7	15.8	27.4
200-499	10,000	84.8	79.5	49.8	18.3	25.8
500 and over	44,590	89.2	87.6	63.9	28.9	37.8
Total	**4,530**	**65.0**	**56.9**	**32.7**	**14.7**	**26.9**

Source: Survey of industrial and service firms (data for 2016 for expenditure and defence measures and data for 2017 for frequency of attacks).
(1) Thousands of euros. – (2) Answers to the question 'Did your company suffer any cyber-attacks in 2017? Consider only attacks that had an effect on the firm's IT system or the integrity and confidentiality of the data stored, including limited or short-lived effects or easily reversible ones.' – (3) The distinction is based on the OECD/Eurostat classification, which distinguishes, in manufacturing, between high-tech and low-tech firms and, in the service sector, between knowledge intensive and less knowledge intensive firms, which for our purposes are likened to their equivalents in manufacturing; within the high-tech category, we distinguish between ICT and non-ICT firms. Energy firms, which were not included in the original classification, are regarded as high-tech non-ICT firms.

As to the type of cyber-defence adopted, two out of three firms report that they provide personnel training on how to use IT equipment securely and over half declare that they carry out analyses of network vulnerability, while just a third encrypt their data, a practice that is less costly than the other two but highly effective. This last fact bears out the hypothesis that there is an information asymmetry working to the advantage of sellers of cyber-defence services, which they exploit to offer firms the most expensive solutions rather than the best ones.

Major differences also exist between sectors and size categories of firm in the adoption of cyber-defence measures and the frequency of attacks capable of impacting on the operation of IT systems or the integrity and confidentiality of the data stored in them. The rate of adoption of defence measures is significantly higher than average among ICT companies and large firms. Data for 2017 indicate that the frequency of attacks is also greater for large firms.

The likelihood of a firm suffering a cyber-attack depends on how attractive it is to hackers, which in turn is linked to the value of the data stored and the firm's exposure to risk (measured, for example, in terms of the number of devices connected to the Internet or the number of transactions conducted online), as well as to its ability to defend itself.

In Italy's production system, the risks appear to be greatest, at present, among high-tech non-ICT firms, because unlike low-tech firms they attract cyber-attacks, but unlike ICT companies they have not acquired sufficient defence capability. This is borne out by the fact that cyber-attacks are more frequent among firms using e-commerce and cloud computing, as well as IoT devices; they occur less often among firms that use AI technologies. The first set of technologies, which are also the most widespread, do not call for advanced technical skills and many of the firms adopting them probably do not try to identify weak points in their security systems and plug them. The use of AI instead demands a higher level of skill (the rate of adoption is seven times higher in the ICT sector than the average for the economy as a whole), which presumably also implies greater attention to cyber-security.

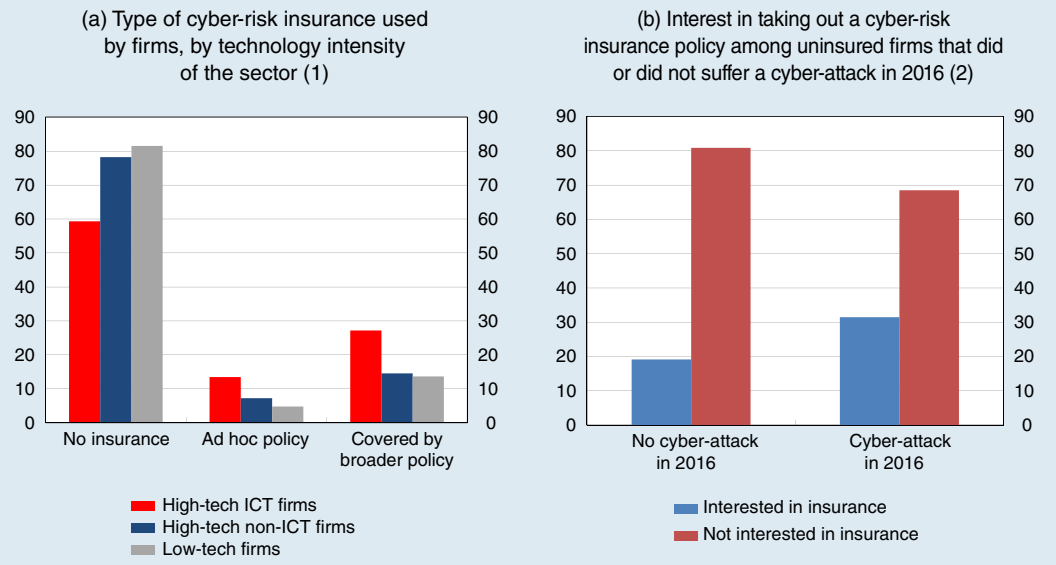
Wide use of specific insurance policies against cyber-attacks could help considerably to mitigate the risk. On the one hand, it would assist in identifying – for legal purposes as well – the liability for any compensation; on the other hand, with appropriately graduated premiums, it would offer an incentive for better management of corporate IT systems, as is already the case in other sectors.[5] The market for cyber-risk insurance is still very underdeveloped, however.

In Italy, about a fifth of firms with 20 or more employees are insured against cyber-attacks, but only a minority of this group have a separate, ad hoc policy, providing greater transparency concerning the scope of coverage and calculation of premiums. As with other aspects of the cyber threat, it is mainly firms in the ICT sector that take out this type of policy (Figure 16.1).

[5] OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 2017.

Figure 16.1

Use of cyber-risk insurance in Italy in 2017
(per cent of firms)



Sources: Business Outlook Survey of Industrial and Service Firms, 2017; Survey of Industrial and Service Firms, 2016.
(1) The distinction is based on the OECD/Eurostat classification, which distinguishes, in manufacturing, between high-tech and low-tech firms and, in the service sector, between knowledge intensive and less knowledge intensive firms, which for our purposes are likened to their equivalents in manufacturing; within the high-tech category, we distinguish between ICT and non-ICT firms. Energy firms, which were not included in the original classification, are regarded as high-tech non-ICT firms. – (2) Firms classified as 'interested' are firms that reported they were not insured because they had not found a suitable policy on the market or because the premiums were too high.

Having experienced a cyber-attack in the past determines in part the amount of interest firms show in seeking cyber-risk insurance, but it also reduces the likelihood that a policy will actually be underwritten. This finding could point to some form of rationing by insurance companies: without sufficiently deep historical data and a fairly rich case history, insurers may use a past event as the main measure of a firm's risk, leaving the latter unable to take out insurance or faced with excessively high premiums. This rationing apparently occurs regardless of the fact that according to the data almost all firms that have experienced a cyber-attack strengthen their defences in its wake.

As to the damage wrought by a cyber-attack, in seven out of ten cases the firms targeted have to allocate additional funds to restore their systems and need to slow their output, even though the actual cost is almost always small. In a few cases, notably those involving ICT companies and firms with more than 500 employees, the damage can be very substantial (Table 16.2).

The policy responses

The increase in cyber-risk has created complex policy challenges for governments. Malware and other means of cyber-attack jeopardize personal and national security and can damage the economy in a similar way to traditional weapons. National legislation and international law are gradually adjusting to the new scenario.

Table 16.2

Technical consequences and financial costs of cyber-attacks
(per cent of firms that reported at least one cyber-attack) (1)

FIRMS	Consequences			Costs			
	Interruption of business	Need to restart systems	Theft or destruction of data	Less than €10,000	From €10,000 to €49,999	From €50,000 to €199,999	More than €200,000
				Sector (2)			
Low-tech	69.5	71.1	16.2	92.4	7.0	0.6	0.1
High-tech, non ICT	72.7	76.9	15.7	92.7	5.7	1.5	0.1
ICT	65.4	72.1	4.6	82.7	15.3	1.8	0.2
				Size class			
20-49	69.9	71.1	15.6	96.6	2.8	0.6	–
50-199	70.4	73.6	14.9	85.6	13.4	1.0	–
200-499	73.3	80.6	17.6	88.6	9.2	2.2	–
500 and over	68.5	78.5	16.9	76.7	18.6	2.4	2.3
Total	**70.1**	**73.4**	**15.6**	**92.2**	**7.0**	**0.9**	**0.1**

Source: Survey of industrial and service firms, 2016.
(1) Data for 2016. – (2) The distinction is based on the OECD/Eurostat classification, which distinguishes, in manufacturing, between high-tech and low-tech firms and, in the service sector, between knowledge intensive and less knowledge intensive firms, which for our purposes are likened to their equivalents in manufacturing; within the high-tech category, we distinguish between ICT and non-ICT firms. Energy firms, which were not included in the original classification, are regarded as high-tech non-ICT firms.

A number of countries began adapting the tools of criminal law in the 1990s by making acts such as unauthorized access to IT systems a criminal offence.[6] Since the early 2000s, the advanced economies and leading emerging countries have been developing broader strategies that usually include the development of an institutional architecture for crisis prevention and management; measures to enhance the security of general government and critical infrastructure; incentives for specialist training and public/private sector cooperation; and software and hardware security certification schemes.

International cooperation projects, which are essential to cope with a global threat, are still few and far between. Progress has been made only on specific aspects, such as the coordination of police forces to combat certain crimes, and in contexts such as NATO and the G7, in which countries share the same main strategic security objectives.

Italy's legislation reflects the cyber-security strategy developed at European level, which rests on Directive EU/2016/1148 (Network and Information Security, NIS). This requires member states to have in place an organization that will make it compulsory for operators of services deemed essential for the economy to adopt stringent security measures. The directive sets up a cooperation group within the EU for the exchange of information and best practices.

[6] For Italy, see Law 547/1993 amending the provisions of the Criminal Code and the Code of Criminal Procedure regarding cybercrime.

IT security requirements for a range of entities are also embodied in two recent EU provisions: Regulation (EU) 2016/679 (the General Data Protection Regulation, GDPR) and Directive (EU) 2015/2366 (the Revised Directive on Payment Services, PSD2). Other obligations may be imposed after the passage of the Cybersecurity Act, presented by the Commission in 2017, which gives the EU the power to certify the security of IT devices and codes.

Italy's cyber-security architecture is set out, for the time being, in two provisions: the Decree of the Prime Minister of 17 February 2017, which tasks the DIS (Department for Intelligence and Security of the Prime Minister's Office) with coordinating the prevention and management of cyber-crises through the Cyber Security Unit (NSC);[7] and the legislative decree transposing the NIS, which makes the DIS the point of contact with European institutions and indicates the authorities in charge of implementing NIS measures in strategic branches of the economy. The competent authority for both the banking industry and financial market infrastructure is the Ministry of Economy and Finance, assisted by the Bank of Italy and the Companies and Stock Exchange Commission (Consob).

The financial system is a key target of cyber-attacks, be they motivated by profit or by the intention to subvert the orderly functioning of the economy. The numerous interdependencies mean that such attacks may cause substantial damage and have repercussions throughout the system. Intensive use of digital technologies also creates multiple potential points of entry for hackers.

Central banks and supervisory authorities have a key role to play in ensuring the cyber-security of the financial system. In many countries they manage vital components, such as payments systems; they can ask supervised entities for information on attacks suffered, call for the adoption of suitable defence measures, and impose sanctions on non-compliance.

International cooperation has achieved better results in the financial sector than in other areas of the economy, although once again there is greater unity among countries in forums like the G7 or the Eurosystem. Convergence on shared guidelines was made easier by previous synergies on other fronts, above all financial stability, and by the global presence of some of the key players. The areas of action include the security of financial intermediaries, on the one hand, and of payment infrastructures on the other (see the box 'International cyber-security initiatives in the financial sector').

INTERNATIONAL CYBER-SECURITY INITIATIVES IN THE FINANCIAL SECTOR

International cooperation on financial sector cyber-security covers three crucial areas: establishing regulatory standards and requirements, developing practices and tools, and preparing risk analysis models for financial stability. It takes place in several venues, reflecting the various levels of sectoral and national competences. The main forum for market infrastructures and payment systems is the Committee on Payments and Market Infrastructures (CPMI) of the Bank for International

[7] The permanent members of the Unit are the ministries forming the Interministerial Committee on the Security of the Republic (CISR): Foreign Affairs, Defence, Interior, Economy and Finance, Economic Development, and Justice.

Settlements (BIS); matters of supervision are dealt with by the Financial Stability Board (FSB) and the BIS's Basel Committee for Banking Supervision (BCBS). The G7 also plays an important role and has published a set of non-prescriptive principles.[1]

The FSB is conducting a study of the regulatory systems and supervisory practices of 25 countries as well as the cyber-security guidelines issued by 10 international organizations.[2] It is also preparing a cyber lexicon, to be published by the end of 2018, which is expected to facilitate future regulatory efforts.

The G7 is drawing up a protocol for international cooperation among authorities to govern responses to cross-border incidents. It has set up a discussion panel with private sector representatives to decide on the best regulatory measures and on methods of exchanging information. One important development will be the creation of a technical frame of reference for a set of exercises to test the effective ability of public and private financial institutions to protect against, register and respond to cyber-attacks, along similar lines to the stress tests already carried out on the banking system.

At EU level, the European Systemic Risk Board (ESRB) ensures high-level liaison on financial stability between the European Commission, the appropriate European authorities,[3] the Eurosystem and the national macroprudential authorities. The European Cyber Risk Group has been set up within the ESRB to analyse the potential systemic impact of cyber-attacks, particularly in respect of the European economy.

In the field of banking supervision, the EBA has issued guidelines for the authorities on the assessment of IT risk and recommendations on the outsourcing of cloud computing services; it has also drawn up security requirements for payment service providers and harmonized supervisory rules. The observance of these requirements by significant banks is monitored within the Eurosystem by the Single Supervisory Mechanism (SSM), which also gathers reports of significant cyber incidents and has set up a specific task force (the Cyber Crisis Group) to handle incidents classified as major. The SSM initiates inspections to analyse cyber-risk in response to specific risk indicators based on incident reports or problems identified during off-site supervision.

Regarding payment systems and other financial market infrastructures, the CPMI-IOSCO working group on cyber resilience (WGCR) is currently monitoring the implementation of the Cyber Guidance issued by the CPMI-IOSCO in 2016[4] and disseminating it beyond the G20 countries. Furthermore, following several

---

1 G7, *Fundamental elements of cybersecurity for the financial sector*, 2016; G7, *Fundamental elements for effective assessment of cybersecurity for the financial sector*, 2017.

2 FSB, *Stocktake of publicly released cybersecurity regulations, guidance and supervisory practices*, 2017.

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

4 CPMI-Iosco (International Organization of Securities Commissions), *Guidance on cyber resilience for financial market infrastructures*, 2016.

serious instances of cyber-fraud,[5] the CPMI recently released a security strategy for reducing the risk of wholesale payments fraud related to endpoint security.[6] In 2017, the Governing Council approved the Eurosystem Oversight Cyber Resilience Strategy for European market and payment infrastructures to harmonize the implementation of the CPMI-IOSCO Cyber Guidance within the EU and to strengthen the readiness of individual financial institutions and their service providers to respond to cyber-attacks. It also promotes cooperation between the public and private sectors and has set up the European Cyber Resilience Board for that purpose.[7]

In 2017, the Bank of Italy set up the GCSC (Gruppo di coordinamento sulla sicurezza cibernetica – Cyber-Security Coordination Group), membership of which is also extended to IVASS (the Italian Insurance Supervisory Authority). The GCSC recently drew up a document detailing the action taken by the Bank and IVASS in the field of cyber-security and how it fits into the international, European and Italian context.[8]

[5] These include cases such as the fraud perpetrated against the Central Bank of Bangladesh in 2016; see BIS, *Central banks are reviewing wholesale payments security*, 2017.

[6] CPMI report, 'Reducing the risk of wholesale payments fraud related to endpoint security', published on the BIS website on May 2018, https://www.bis.org/press/p180508.htm.

[7] Cyber Resilience Oversight Expectations (CROE) are now being drawn up, along with a plan for advanced cyber-security testing (EU Threat Intelligence Based Ethical Red Teaming, TIBER-EU); ECB, *Views on the regulation of cyber security*, 2017.

[8] GCSC, *Documento quadro sul rischio cibernetico*, forthcoming.

The cyber-security policies adopted in the advanced economies assign the exchange of information between the public and private sector a key role in preventing and responding to cyber-attacks. However, those who have been the victim of an attack or who have identified weak points do not always share what they have learnt because they are unsure about confidentiality and reciprocity. Sometimes favourable conditions occur spontaneously within groups of economic agents that are highly aware of cyber-risk. More often the authorities need to step in to provide encouragement and establish trust: the financial sector has developed advanced solutions in Italy as well (see the box 'The computer emergency response teams (CERT) in the Italian financial sector).

THE COMPUTER EMERGENCY RESPONSE TEAMS (CERTS) IN THE ITALIAN FINANCIAL SECTOR

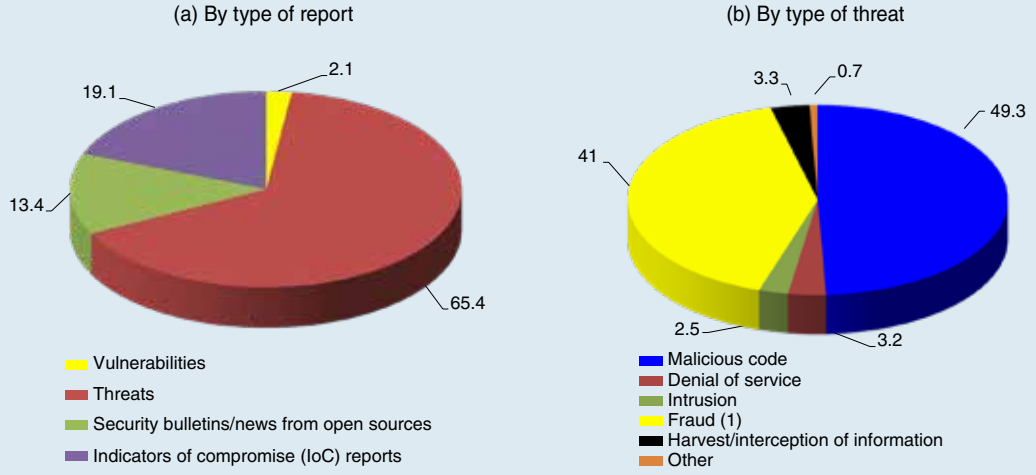
There are two prevailing models for sharing information on computer security incidents: information sharing and analysis centers (ISACs), which are platforms that enable participants to interact but lack a system for joint response; and CERTs and computer security incident response teams (CSIRTs), which enable both the sharing of information and the rapid coordination of responses to any incidents. There are also international and European CERT/CSIRT cooperation networks that comply with specific quality standards.[1]

[1] The main CERT/CSIRT networks are: the Forum of Incident Response and Security Teams (FIRST), active since 1990, bringing together more than 300 organizations from different countries and sectors; and the Trusted Introducer, formed by the community of European CERTs in 2000, which has over 100 member organizations.

Italy's regulatory framework[2] envisages the creation of a CERT/CSIRT network that unites the general government sector with operators of essential services and of critical national infrastructures (for example, the electricity grid, and telecommunications and transport networks); it also encourages the development of cohesive sectoral strategies. In this respect the Bank of Italy and the other authorities perform the dual role of regulators and promoters of public-private partnership initiatives for sharing information.

The Bank of Italy has bolstered its ability to withstand cyber-attacks by forming an internal CERT that participates in international cooperative networks and provides a wide range of security services to the Bank itself (CERTBI). The primary objective is to enhance the Bank's ability to analyse cyber-threats in order to develop effective preventive mechanisms. Specifically, CERTBI oversees training programmes designed to raise the cyber security awareness and the risk culture both of the Bank's employees and external stakeholders.

CERTFin Reports
(per cent)



Source: CERTFin. Data updated to 31 December 2017.
(1) Unauthorized use of resources, phishing, attacks designed to misappropriate money from customers.

The Italian financial sector CERT (CERTFin) has been in operation since January 2017. It was developed as a joint initiative of the Bank of Italy and the Italian Banking Association (ABI) to enhance the exchange of information within the national financial sector. Its members comprise 42 financial institutions (36 banks and banking groups, Poste Italiane SpA, four technical service providers and an operator of financial market infrastructures).[3] In its first year of operation, CERTFin analysed and sent to its members around 1,000 reports on possible attacks, breaches

[2] Directive on national cyber protection and digital security (DPCM of 17 February 2017) and Directive (EU) 2016/1148 on the security of networks and information systems.

[3] The Bank takes part in both the governing bodies (strategic and steering committees) and operational activities (through CERTBI).

and technological vulnerabilities, of which more than two thirds were on threats of attacks (see panel (a) of the figure), specifically campaigns to spread malware and attempted fraud, such as phishing (see panel (b) of the figure).

As part of its efforts to raise cyber security awareness it has also published a pamphlet containing guidelines for the safe use of online banking, payment cards and e-commerce services. Finally, CERTFin belongs to the international networks of CERTs, broadening the opportunities for exchanging information to the benefit of its members.

The measures described above are a step in the right direction but they are not enough. They apply only to certain sectors (like the NIS directive) or specific types of attack, however frequent (like those envisioned in the GDPR). There are still no principles of civil liability that can rectify the externalities at a more general level.