BANCA D'ITALIA
EUROSISTEMA

Cybersecurity in the financial sector: role of authorities and value of cooperation

Opening speech by Paolo Angelini
Deputy Governor of the Bank of Italy

Conference "Public-private cooperation for the cyber resilience of the Italian financial sector - Opportunities for operators and the role of CERTFin"

Rome, July 4, 2024

Ladies and gentlemen, it is a pleasure for me to welcome you at the Bank of Italy for this conference, which addresses issues whose relevance has been rapidly growing in recent years.

The digitalization of services, and of social relations themselves, is now a structural element of the context in which we live. In the field of financial services the phenomenon has developed in advance relative to other markets. It has brought significant benefits, but also new operational risks, which have grown rapidly recently. Both the increase in online use of certain financial services induced by the pandemic and the tendency to use cyberspace as a place of aggression for political, economic or purely criminal purposes have contributed to this, also as a result of the recent escalation of international tensions.

The authorities, associations, intermediaries present at this conference are all on the front line, each in their own area of competence, to define rules, strategies and tools to counter these risks and contribute to the safe development of the digital ecosystem.

In my remarks I will mention recent developments in cyber incidents, I will illustrate some key upcoming regulatory innovations, I will underline the importance of cooperation between institutions and intermediaries in the fight against cybercrime.

Cyber attacks increase and response actions diversify

Cybercrime evolves rapidly. It adopts increasingly sophisticated techniques and tools, takes multiple forms (from ransomware to online fraud), attacks heterogeneous subjects (citizens, companies, public and private organizations).

The spread of the Crime-As-a-Service paradigm allows even subjects with limited technical, financial or organizational capabilities to purchase or outsource the

necessary services to conduct effective illegal activities in cyberspace. Cyber criminals themselves benefit from technological progress: developments in artificial intelligence and, prospectively, quantum computers, offer new opportunities for economic and social development, but can also be used to undermine the prevailing security mechanisms.

According to a survey by the Bank of Italy on industrial and non-financial private service companies with more than 20 employees (INVIND 2023, collecting 2022 data), almost 90 percent of companies are aware of the possibility of suffering a cyber attack. Those who have been victims of an attack perceive a higher risk, which is associated with greater investment in prevention. Smaller companies, with a number of employees between 20 and 49, are less aware of cyber risks: those who consider it not at all likely that a cyber attack could affect a company with their same characteristics are 14 percent of the sample, compared to 7 percent among companies with more than 50 employees.[1] It is therefore not surprising that attacks on companies' computer systems mainly target larger ones, which have greater economic capacity, but also exploit the lesser degree of preparation that characterizes medium or small-sized companies (SMEs).

The annual report of the National Cybersecurity Agency (ACN) documents a strong increase in reported incidents in 2023 (303, compared to 126 in 2022), which has affected all economic sectors.[2] The number of ransomware-type attacks, which is the most alarming phenomenon, has increased by 27 percent, affecting both SMEs and large companies. For SMEs the phenomenon is likely underestimated, given that these companies are often without adequate cybersecurity defenses and tend not to report incidents. Similar trends have also been recorded at European and international level.[3]

The financial sector is a privileged target for cybercriminals due to its high technological intensity, strong interdependence among financial community operators at both national and global levels, and the economic and strategic value of the functions it performs. Reports sent to the Bank of Italy by banks and payment service providers confirm a significant acceleration in the number of cyber incidents last year: 30 reports of attacks, compared to 13 in 2022 (fig. 1.a). The most frequent cases concerned the availability of services offered to customers (so-called Denial Of Service attacks; fig. 1.b), sometimes carried out by subjects that appear to be related to governments of non-European countries.

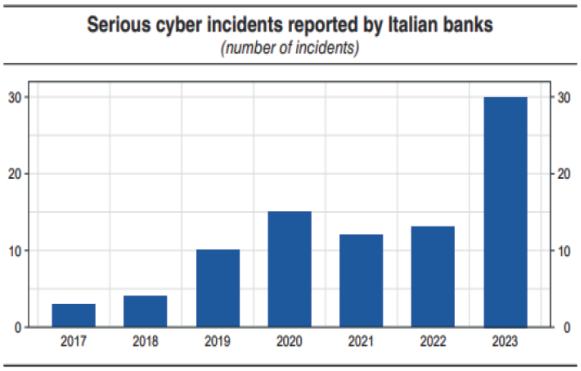
---

1 See L. Bencivelli and M. Mongardini, "La sicurezza cibernetica delle imprese italiane: percezione dei rischi e pratiche di mitigazione, Bank of Italy, Occasonal paper series, 852, June 2024, https://www.bancaditalia.it/pubblicazioni/qef/2024-0852/index.html?com.dotmarketing.htmlpage.language=1

2 See National Cybersecurity Agency (ACN), Annual Report to Parliament, 2023, https://www.governo.it/en/articolo/presentation-national-cybersecurity-agency-s-annual-report-parliament/25514

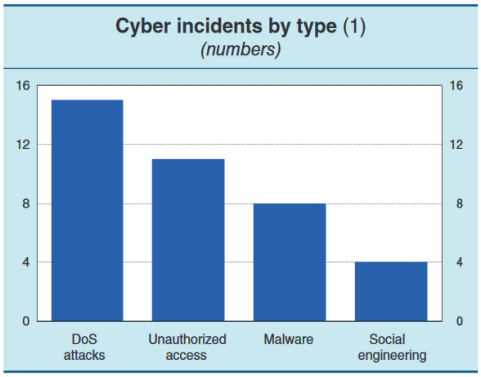
3 See European Union Agency for cybersecurity, ENISA Threat Landscape 2023; International Monetary Fund, Global Financial Stability Report, April 2024.

Figure 1.a



Source: Supervisory reports.

Figure 1.b



Source: Based on supervisory reports.
(1) An incident can be classified into more than one type. Data for 2023.

The growth of cybercrime is countered by actions on two fronts. On one hand, essential defensive measures are taken by potential victims, adapting strategies, governance structures, and investments in technology, resources, processes, and training. On the other hand, cooperative efforts involve law enforcement, regulatory authorities, and potential victims of the threat – including businesses and various public entities (today's meeting is part of this effort). Financial authorities also collaborate internationally, promoting the adoption of shared rules, policies, control tools, and initiatives.

The Bank of Italy is engaged in this process both due to its institutional role in safeguarding financial system stability and as the manager of critical infrastructure for the country and the Eurosystem. Our strategic planning includes actions that cover both fronts.

Preparing for regulatory innovations

The main novelty coming in the legislative field is represented by the DORA (Digital Operations Resilience Act), which will come into force in January 2025 and will comprehensively regulate digital operational resilience in the financial sector.

Although introducing various elements of novelty, for numerous aspects DORA moves in continuity with the past. For example, some provisions were already applied to the financial sector in the form of guidelines.[4] Furthermore, IT risk has long been an integral part of the SREP (Supervisory review and evaluation process), which provides for in-depth analyses and targeted inspections and includes the setting of capital requirements for intermediaries.

The provisions regarding so-called 'third parties' (entities that provide technology and digital services to the financial sector) introduced by DORA are not entirely new. Some powers of supervisory and regulatory authorities toward these subjects were already

[4] See European Banking Authority (EBA), Guidelines on ICT and Security Risk Management https://www.eba.europa.eu/guidelines-ict-and-security-risk-management

present in the national legal system for several years[5]. The Regulation extends and strengthens these powers with the introduction of a new surveillance regime on critical suppliers at the European level, which will be identified based on qualitative-quantitative criteria.

DORA introduces specific provisions regarding TLPT (Threat Led Penetration Test), exercises that must be conducted by all major banks, market infrastructures, and European insurance companies. These exercises allow the intermediary to verify its level of resistance and resilience in the face of a specific cyber threat scenario. Although this tool was already known in many jurisdictions, including Europe, the regulation now structures its use more systematically, with the participation of both authorities and external specialists.

Finally, DORA promotes the participation of financial entities and supervisory authorities in information-sharing mechanisms, emphasizing cooperation and the development of public-private initiatives such as our sector CERT, CERTFin.

The drafting of secondary regulations connected to the primary legislation is nearing completion. The Bank of Italy has participated with other competent authorities, both Italian and European, in finalizing the texts and is now focusing on the impacts in terms of processes, methodologies, and necessary resources for implementation.

One aspect we are closely monitoring is the consistency of this regulatory framework with rules related to network and information system security, which are also undergoing significant revision with the upcoming implementation of the NIS2 Directive. We are collaborating with relevant institutions, including the Ministry of Economy and Finance (MEF), the National Cybersecurity Agency (ACN), and the Prime Minister's Office, to avoid uncertainties in application and duplications of burden for operators.

The importance of cooperation

Individual countermeasures, regulation, and supervision, even if strengthened, are not enough to protect the sector from increasingly sophisticated and insidious threats. Cooperation among the various actors involved allows for the promotion of awareness regarding risks associated with the most innovative technologies, timely identification of threats, and activation of the most effective remedial actions.

In this context, cooperation among financial intermediaries, far from representing a threat to market competitiveness, constitutes an essential risk mitigation tool. The Bank of Italy has always promoted these forms of cooperation in areas where the decisions of individual intermediaries alone cannot achieve optimal results. Through its own

---

5 Since 2015, supervisory and regulatory authorities have specific powers over non-supervised subjects to whom different types of financial entities have outsourced business functions. The Bank of Italy can request information (in some cases based on contracts signed between the supervised subject and the provider) and conduct inspections, summon administrators and other personnel, and apply sanctions in case of non-compliance with requests.

CERT (CERTBI), the Bank collaborates with various actors operating within the national cybersecurity architecture, including the National Cybersecurity Agency (ACN), as well as the State Police, the Carabinieri, and the Guardia di Finanza. Similarly, through the financial sector's CERT, CERTFin, established in 2017 together with ABI (the Italian Banking Association), we address new risks collectively.[6] The experience of these seven years of operation has been overwhelmingly positive, as evidenced by the growth in the number of participants (from approximately 20 to the current 70), a significant increase in information exchanges, and the strengthening of collaboration networks with similar international organizations.

Cooperation with entities outside the financial world is also crucial. Cyberspace knows no boundaries, and cybercriminal attack techniques do not discriminate based on the victim's sector. In our country, a systemic approach has been made possible in recent years through the adoption of a National Cybersecurity Strategy and the cross-cutting role assigned to the National Cybersecurity Agency (ACN). Similarly, European legislation has outlined a path of collaboration among institutions in essential sectors of society and the economy through the NIS Directive.

Despite these advancements, some challenges remain. The multitude of initiatives in this field highlights a complex and sometimes fragmented framework, necessitating increased coordination and operational alignment among all involved institutions. This structure presents coordination difficulties and relatively high costs.

This topic will be discussed today, and we hope to derive valuable insights for improvement.

In this context, I am pleased to announce that today, following the first roundtable, a Memorandum of Understanding will be signed between CERTFin and the Central Directorate for Scientific Police and Cybersecurity of the Ministry of the Interior. This underscores our joint commitment to enhancing the safety of the digital financial services ecosystem for the country and its citizens.

6 See https://www.certfin.it/

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