

# DIGITAL RESILIENCE IN THE ITALIAN FINANCIAL SECTOR: EVIDENCES FROM THE SUPERVISORY INCIDENT REPORTING FRAMEWORK



# DIGITAL RESILIENCE IN THE ITALIAN FINANCIAL SECTOR: EVIDENCES FROM THE SUPERVISORY INCIDENT REPORTING FRAMEWORK

The work has been authored by Fulvio Di Stefano, Sebastiano Russo, Benedetto Andrea De Vendictis and Luca Cusmano.

The data presented are collected exclusively for supervisory purposes and are processed in aggregate form in compliance with privacy legislation.

The authors would like to thank Valentina Cappa and Alessio Orlandi for some constructive and critical discussion.

### © Bank of Italy, 2024

### Address

Via Nazionale 91 00184 Rome - Italy

### Website

http://www.bancaditalia.it

All rights reserved. Reproduction is permitted for educational and non-commercial purposes, provided that the source is cited.

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

# **INDEX**

Lis	t of ac	ronyms		4
AB	STRA	CT		5
1	INT	RODUC	TION	6
2	EVII	DENCES	FROM REPORTED INCIDENTS	7
3	MOS	ST COM	MON ROOT CAUSES OF THE INCIDENTS	9
	3.1	Operat	cional incidents	9
	3.2	Cyber	incidents	10
		3.2.1	Social engineering campaign towards intermediaries	11
		3.2.2	Ransomware and data breaches campaign	11
		3.2.3	DDoS attacks	12
4	IMP	ACTS O	F REPORTED INCIDENTS	12
5	CON	NCLUSIO	ONS	14

## List of acronyms

DDoS: Distributed Denial of Service

DORA: Digital Operational Resilience Act

EBA: European Banking Authority

ECB: European Central Bank

EIOPA: European Insurance and Occupational Pensions Authority

ENISA: European Union Agency for Cybersecurity

ESMA: European Securities and Markets Authority

EU: European Union

FSB: Financial Stability Board

ICT: Information and Communication Technology<sup>1</sup>

IMF: International Monetary Fund

IT: Information Technology<sup>1</sup>

PSD2: Payment Services Directive 2

SSM: Single Supervisory Mechanism

TPP: Third-Party Service Provider

<sup>1</sup> The two terms are used interchangeably.

### **ABSTRACT**

This paper presents statistics and evidences derived from the Italian operational or security incident reporting framework established by Banca d'Italia for banks and other financial institutions since 2015. The number of reported major operational or security incidents is rising over the years in the Italian financial market. This is a consequence of both the growing digitalisation of financial services and a reduction in the under-reporting phenomenon, which still represents a major hindrance for effective microprudential and macroprudential assessments. The evidences show an increasing involvement of third party service providers in reported incidents. Notwithstanding, the resilience of the Italian financial market has appeared adequate, with limited impacts on the entities. If promptly and adequately implemented, the novel regulatory actions to address the challenges arising from technological risk will improve the effectiveness of the supervisory tools.

### 1 INTRODUCTION

The increasingly widespread use of information technologies is a factual trend in the banking sector. On the one hand, technological evolution can bring significant benefits in terms of management of services, investments profitability and improvements in customer satisfaction. On the other hand, the possibly inadequate usage of information systems and the growing cyber threats pose risks for the stability of individual intermediaries and the financial system as a whole. Therefore, banking and financial supervision has long recognized the increasing importance of addressing technological risk (also referred as IT risk), up to the point that it has become a strategic priority both at national<sup>2</sup> and European<sup>3</sup> level.

Incident reporting is widely regarded as a key tool for assessing both the microprudential and macroprudential aspects of IT risk.<sup>4</sup> The reporting of major operational or security incidents allows, from a supervisory perspective, to:

- support prudential supervisory assessments of individual intermediaries, as incidents are a key indicator in the assessment of operational risk;
- coordinate and provide support for remediation actions, particularly in the case of incidents involving multiple operators;
- assessing systemic trends against new threats and vulnerabilities common to the financial market in a timely manner;
- strengthen "information sharing" processes within the financial system.

Banca d'Italia manages an incident reporting framework that requires banks, payment institutions and electronic money institutions (hereafter financial entities) to report major operational or security incidents.<sup>5</sup> An incident is defined as a singular event or a series of linked events, unplanned by the financial entity, which have or will likely have an adverse impact on the integrity, availability, confidentiality and/or authenticity of services.

When an event occurs, Italian financial entities classify operational and security incidents as "major" if they meet the criteria and thresholds defined by Banca d'Italia (depending on the type and size of the intermediaries) and report all major incidents to Banca d'Italia in a timely manner.6

The Italian reporting framework perimeter includes incidents related to both malicious activity (hereafter called cyber incidents) and operational events (e.g.,

<sup>2</sup> Banca d'Italia, Piano Strategico per il triennio 2023-2025.

European Central Bank, SSM supervisory priorities 2024-2026.

European Central Bank, IT and cyber risk – the SSM perspective 2019.

The framework has been established in 2015 for banks, with updates to the Circular No. 285 (the act ruling the banking and financial supervision in Italy) and in 2017 for payment institutions and electronic money institutions, with updates to the Supervisory Provisions for these institutions.

Banca d'Italia, Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza.

malfunctions), being integrated with the two EBA<sup>7</sup> and ECB/SSM frameworks<sup>8</sup> defined at European level. In particular, the EBA framework, established following the entry into force of PSD2, applies to all financial entities but is limited to incidents (both malicious and non-malicious) impacting payment services; the ECB/SSM framework, established in 2017, applies only to significant institutions and refers only to cyber incidents.

The objective of this report is to provide an overview of IT risk from a supervisory perspective. Chapter 2 presents statistical data and major trends on the reported incidents. Chapter 3 describes the main root causes of the incidents observed in the Italian banking industry with their impacts outlined in chapter 4. Finally, chapter 5 discusses the evidences presented and provides some concluding remarks.

### 2 EVIDENCES FROM REPORTED INCIDENTS

The upcoming evidences refer to data collected in the period spanning from 2020 to 2023. The number of financial entities subject to the incident reporting framework during 2023 is shown in Table 1. The data have remained stable in the analysed period, with the majority of entities being banks or banking groups and a minor part being payment institutions and electronic money institutions.

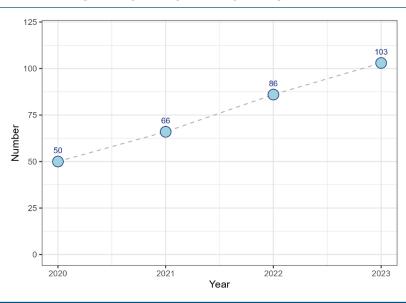
		Table 1		
FINANCIAL ENTITIES SUBJECT TO THE INCIDENT REPORTING FRAMEWORK DURING 2023				
FINANCIAL ENTITY	NUMBER			
Italian significant banks or banking groups				
Branches of non-EU banks or banking groups	8			
Subsidiaries of EU banks or banking groups				
Italian less significant banks or banking groups				
Payment institutions	43			
Electronic money institutions	10			

Figure 1 shows that the number of reported major operational or security incidents with impacts in Italy has continuously increased in the last years. The number of reported incidents in 2023 has more than doubled with respect to 2020. At the same time, the number of entities that reported at least one incident has risen (12% in 2020, 19% in 2021, 29% in 2022 and 26% in 2023).

<sup>7</sup> European Banking Authority, Revised Guidelines on major incident reporting under PSD2 of 7 March 2017 and subsequent updates.

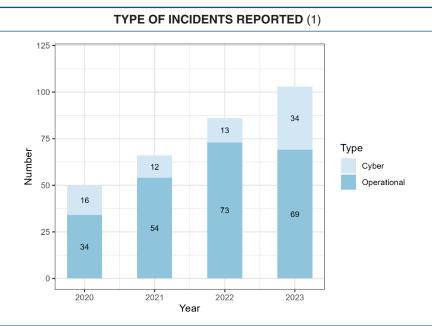
 $<sup>8 \</sup>quad \text{European Central Bank, } \textit{IT risk-ECB to roll out cyber incident reporting framework 2017}. \\$ 

### NUMBER OF REPORTED INCIDENTS IN ITALY



Operational incidents represent the greater part of the events, the rest being cyber incidents (see Figure 2). While operational incidents experienced an increase from 2020 to 2022 and a slight decrease in 2023, cyber incidents experienced a decrease from 2020 to 2021, then remained stable in 2022 and increased in 2023. This latter trend can possibly be explained by the impacts of the Russo-Ukrainian war and the consequent geopolitical conflicts.

Figure 2



(1) Cyber incidents include both cyber attacks and other incidents classified as cyber in the incident reporting framework, such as accidental data leakages.

An increase in the number of incidents involving third-party service providers (TPPs) has also been experienced. In Figure 3 it is possible to see that the percentage of incidents involving third-parties has been stably around 50% over the years when it comes to operational incidents, while the percentage of cyber incidents involving a TPP, lower in 2020 and 2021, has been comparable to operational incidents in 2022 and 2023.

THIRD-PARTY PROVIDER INVOLVEMENT IN REPORTED INCIDENTS

Figure 3



2022

2023

### 3 MOST COMMON ROOT CAUSES OF THE INCIDENTS

Year

2021

### 3.1 Operational incidents

2020

As noted above, the greater part of reported incidents is operational. The main cause of these incidents is systems malfunctioning and the vast majority are software failures, mainly connected to malfunctions/bugs and incorrect update operations or application modifications. The rest regards hardware failures, mainly referring to connectivity and/or network equipment problems. Various cases of operational incidents related to poor ability of the systems to adequately manage operational peaks were noted, for example in the event of an increase in traffic generated by users. Incidents related to human errors and internal processes are also reported.

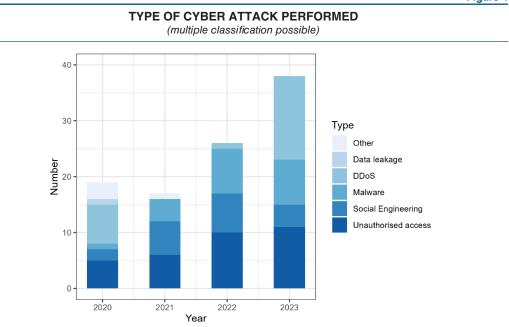
During 2023 a specific analysis was conducted to better assess the impacts of the risks related to the change management processes (so-called ICT change risk) on the Italian market. Evidence shows that inadequate hardware and software change processes are the primary cause of unavailability events for most significant Italian banks, and approximately 40% of incidents reported by such entities in the Italian market originate from issues related to ICT change management processes. The most common problems are attributed to human errors and incorrect system configurations.

The primary strategies to mitigate ICT change risk and consequently minimize the occurrence of operational incidents typically involve process automation, application of the 4-eyes principle, additional monitoring activities and evolution of the testing phases to closer to real life scenarios.

### 3.2 Cyber incidents

Cyber attacks reported by financial entities in the incident reporting framework are complex and frequently involve multiple attacking techniques. Figure 4 illustrates the type of cyber attack performed. The most common include unauthorised access, social engineering and malware. Notwithstanding, 2020 and 2023 have experienced an increase in reported DDoS attacks, the latter mainly due to a campaign prosecuted by pro-Russian hacktivists in response to the Italian support to Ukraine in the conflict.

Figure 4



Some critical issues in the defence measures against cyber attacks have been identified in recent years. These include:

- · Limited level of security awareness among employees with specific reference to risks emerging from social engineering attacks;
- · Management of remote access applications and/or procedures for remote access to workstations not always adequate (e.g., presence of unplanned remote access tools, identification of operators before granting remote access, single factor authentication procedure);
- · Application configurations not always adequate (e.g., storage of credentials in the browser);

- · Inadequate risk assessment processes (e.g., branch computer applications operational even while they are closed, inadequate physical security on the entities' premises);
- · Lack or imperfect application of the anti-DDoS systems, including the lack of coverage towards some internet facing applications and the lack of appropriate stress-testing of the defence measures in place;
- · Delays in the patching processes.

One important addition is that financial entities are not the sole objective of criminals: service providers have been the target of numerous supply chain attacks. In these cases, mitigation actions aim to strengthen and improve the security of the supplier's systems from a technical and organizational perspective. Staff training and awareness-raising activities are required, alongside the adoption of specific suitable technical measures on the IT infrastructure and organizational safeguards with respect to internal processes.

With the aim of providing some case studies, below are presented three examples of cyber attack campaigns conducted in recent years, where similar modus operandi by the attackers has been identified.

## 3.2.1 Social engineering campaign towards intermediaries

In recent years, some similar social engineering events have been perpetrated against financial entities. The objective is to obtain remote access on the employees' workstations. If the remote access is secured, the attacker tries to locate internal management applications and to complete his malicious activity by entering fraudulent transfers or modifying some customer data for home banking access. These malicious activities are conducted during both day time and night time hours, in case employees leave the PC on and connected even in their absence or there is no time limitation or time controls on the usage of applications. In some cases, additional social engineering techniques were used to guarantee the acceptance of fraudulent transfers.

The economic impacts of the campaign are found to be substantially contained (see chapter 4), especially thanks to the already implemented anti-fraud systems and/or SOC monitoring activities. However, some intermediaries reported significant peaks of operational losses, which, however, have not affected clients.

### 3.2.2 Ransomware and data breaches campaign

Several reports refer to TPPs and intermediaries who are victims of a ransomware campaign. The attack usually begins by exploiting phishing techniques that allow criminals to break into the entity/provider's systems. Through subsequent lateral movements, the attackers are able to encrypt either the entire system or a portion of it. If the attack is successful, a ransom is demanded to unlock the encrypted systems. The

attackers, following the unauthorised access, try to attempt a double extortion. If they are able to steal some data from the accessed systems, they demand another ransom to avoid the publication of the exfiltrated data on the (dark) web.

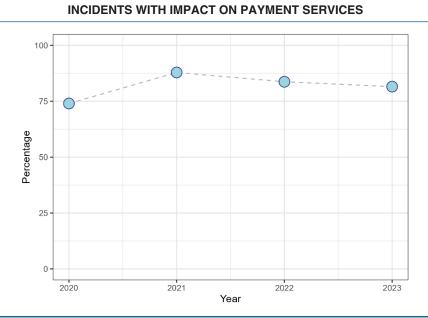
### 3.2.3 DDoS attacks

Financial entities have also been targeted by DDoS attacks, which are designed to disrupt service availability by overwhelming systems with an excessive volume of requests, without waiting for responses. During such attacks, intermediaries typically employ primary defence measures, including blocking requests originating from the user-agent that initiates the attack, blocking the primary IP addresses used in the attack, or even blocking all requests from the country where the attack originates. Recent attack patterns have also revealed the involvement of various geographical sources in initiating flooding, making traditional countermeasures less effective.

### 4 IMPACTS OF REPORTED INCIDENTS

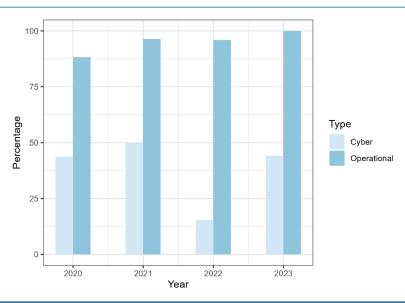
From 2020 to 2023 the percentage of incidents impacting payment services (including ATMs, web banking, mobile banking, points of sales) has ranged from 74% to 88% (see Figure 5). These, being online and time-sensitive services, are subject to frequent evolutions and are, therefore, particularly exposed to incidents.

Figure 5



As a matter of fact, Figure 6 shows that operational incidents almost entirely affect payment services, a trend which has remained stable in the last years. On the other hand, the percentage of cyber incidents involving payment services is much lower.

### INCIDENTS WITH IMPACT ON PAYMENT SERVICES BY TYPE



An in-depth analysis on the 2023 data shows that the disruption of service availability and continuity is the main consequence of incidents and characterizes all types of intermediaries. Overall, 80% of incidents have resulted, to varying degrees, in the interruption or slowdown of a service, whether it is a payment service, a core banking service, or ancillary service.

Taking into account just the incidents with impacts on the availability of services, the analysis shows that:

- Incidents result in an average of approximately 9 hours of service interruption or slowdown. However, incidents impacting critical services (such as online banking, ATMs, etc.) and potentially affecting a significant number of clients (i.e., over 100,000 clients) have a shorter average recovery time of approximately 5 hours, or 3.5 hours considering significant institutions only;
- · Cyber incidents have generally below-average impacts on availability, except for very few cases;
- Only 4 reported incidents have resulted in unavailability of services for more than one day. However, two of them were resolved within two days and impacted no more than 50,000 clients, and the other two impacted non critical services.

The economic impact of incidents is usually negligible. Only on 2 occasions in 2023 the threshold for classifying the incident as "major" under the "economic impacts" criterion 10 was exceeded.

Most incidents are closed<sup>11</sup> within 24 hours, with the vast majority being closed within a week. However, there are some incidents which take longer to be resolved. Those are mostly cyber incidents, for which operators typically conduct longer investigations and the closing time occurs when the analyses are concluded rather than when operations return to normal.<sup>12</sup>

### 5 CONCLUSIONS

The data presented in earlier chapters highlight an increasing trend in the number of incidents reported to Banca d'Italia over the years. Operational incidents are the vast majority, while cyber incidents have seen a sharp rise in recent years, as observed both by the ENISA<sup>13</sup> with respect to the incidents reported at EU level and by the IMF<sup>14</sup> with respect the incident reported at global level. Operational incidents primarily involve systems malfunctioning, hardware failures, human errors and inadequacies of internal processes. Unauthorised access, social engineering, malware and DDoS are the most reported cyber attacks, in line with the prominent threats identified at EU level. The most common root cause of operational incidents is often found in shortcomings within ICT change management processes. On the other hand, cyber incidents are mainly caused by inadequacies in: the level of security awareness among employees, the management of remote access, the application configurations, the risk assessment processes, the application of the anti-DDoS systems and the patching processes. Approximately 50% of incidents involve a TPP in 2023, due to an increment in their involvement in cyber incidents over the years and a steady rate for operational ones. The impacts of the incidents mainly concern the disruption of service availability and continuity, in particular of payment services. However, limited impacts have been reported and, in line with the data reported globally, losses for financial entities have been contained, with sporadic exceptions.

The evidences from this report outline some fundamental points for financial supervision. On the one hand the relevance of the incidents involving TPPs is

<sup>9</sup> Within the incident reporting framework, economic impact refers to the total amount of losses, both direct and indirect, expressed in euros. Costs to be considered include, purely as examples, hardware and/or software replacement costs, penalties for contractual breaches, lost revenues, etc. In the aftermath of the incident detection, accurately quantifying the economic losses can be challenging and, therefore, the intermediary provides rough estimates. These estimates are gradually refined in subsequent incident updates, but in some cases the actual quantification may occur long after the incident closure or may not occur at all (e.g., regarding potential legal expenses, lost revenues due to missed business opportunities, etc.).

<sup>10</sup> The economic impact criterion requires that the estimated financial impact of the incident is above the maximum between the 0.1% of the common equity tier 1 capital and 200.000 euros, or 5 million euros.

<sup>11</sup> According to the incident reporting framework, an incident is considered closed when normal operations have been restored and activity has returned to normal.

<sup>12</sup> Usually a cyber incident is considered closed when all analyses have been concluded and has been ensured that all impacts have been adequately assessed.

<sup>13</sup> ENISA Threat Landscape 2023, 19 October 2023.

<sup>14</sup> International Monetary Fund Global Financial Stability Report. The Last Mile: Financial Vulnerabilities and Risks, 16 April 2024.

evident. These may represent a systemic risk given the constantly increasing level of interconnections between the intermediaries and the third-parties. With the ongoing trend towards specialization and learning economies, there is a significant proliferation of outsourced services that causes financial entities to share common TPPs, software solutions and hardware components. Consequently, financial entities themselves and the third parties they rely on are required to adopt appropriate ICT industry standards to protect their systems. This last fact questions the providers' ability to appropriately manage ICT systems while not being subject to direct oversight and highlights that it is therefore critical for intermediaries to ensure that risks arising from any third party are adequately and effectively identified, assessed, measured, managed and monitored. The novel regulations discussed below may help in partially addressing such issues.

On the other hand, the uprising trend in the number of reported incidents could be attributed to both an increased occurrence of incidents due to greater reliance on ICT systems by intermediaries and a reduction in under-reporting. The latter phenomenon refers to the lack of complete reporting of major operational or security incidents to the competent authorities. Such behaviour can result in the acquisition of incomplete and fragmented information by supervisory authorities, thereby hindering effective microprudential and macroprudential assessments. As a matter of fact, the trends and the evidences presented in the earlier chapters are based on the reports sent by financial entities themselves and, therefore, the analyses conducted might also be influenced by under-reporting. To improve the data quality of the collected information and, as a consequence, effective supervision and financial stability analysis, appropriate reporting of cyber incidents to supervisory agencies has to be strengthened. Horizontal targeted reviews, deep dives and on-site campaigns are in line with this strengthening requirements and can help in reducing the phenomenon, which may be otherwise difficult to detect by using exclusively off-site supervisory tools. At the same time, competent authorities are aiming to enhance their communication channels with intermediaries, clarifying their intentions and outlining the advantages of comprehensive reporting for supervised entities.

The topic of incident reporting has emerged as a key tool for the supervision on IT risk. Therefore, it is the subject of several initiatives at the international level. One of the major concerns regards the harmonization of the fragmented reporting schemes to which intermediaries are subject. This lack of harmonization can hinder supervisors' ability to identify emerging threats promptly and can lead to delays in communication among different competent authorities involved. At the G20 level, the FSB Cyber Incident Reporting Working Group has published in April 2023 a set of documents<sup>15</sup> seeking to address the existing fragmentation in reporting schemes and promote harmonization across different frameworks, with completion expected by 2025.

At the EU level, the Digital Operational Resilience Act<sup>16</sup> (DORA) introduces a novel operational or security incident reporting framework. The main objective

<sup>15</sup> FSB sets out a comprehensive approach to achieve greater convergence in cyber incident reporting, 13 April 2023.

<sup>16</sup> Regulation (EU) 2022/2554 of the European Parliament and of the Council, 14 December 2022.

of DORA is to achieve harmonization by implementing standardized taxonomies, templates, and procedures shared among the three European sector supervisory authorities (EBA, ESMA, and EIOPA). Additionally, DORA assigns the responsibility to these authorities, along with the ECB and ENISA, to propose the establishment of a European Hub for centralized reporting collection. DORA also emphasizes the need for financial entities to develop strategies to address cyber risks arising from third parties and to maintain control over their operational risks, information security and business continuity in their contractual agreements. Furthermore, recent updates to supervisory regulations now extend certain regulatory requirements, previously provided only for outsourcing, to third-party contracts as well. As a result of these updates, intermediaries are required to ensure that their contracts with technology service providers incorporate minimum cybersecurity standards and include specifications on the lifecycle of the intermediaries' data.

Competent authorities need to promptly and adequately implement the contents of the novel regulations and policy documents in order to harmonize existing regulation and improve the effectiveness of the supervisory tools. This would allow to increase the awareness of the intermediaries on the topic, while, at the same time, improving supervisors' ability to address the phenomenon, thereby strengthening financial stability.