BANCA D'ITALIA
EUROSISTEMA

Framework segnaletico di Vigilanza degli incidenti operativi o di sicurezza

Analisi orizzontale 2024

Giugno 2025

BANCA D'ITALIA
EUROSISTEMA

Framework segnaletico di Vigilanza degli incidenti operativi o di sicurezza

Analisi orizzontale 2024

Giugno 2025

Questo documento è stato redatto da Luca Cusmano, Valentina Cappa, Fulvio Di Stefano e Giulia Arangio.

I dati utilizzati nelle analisi sono stati raccolti a fini di supervisione e sono stati trattati ed elaborati in forma aggregata nel rispetto della normativa sulla privacy.

Gli autori ringraziano i colleghi del team di gestione incidenti della Divisione Supporto Statistico e Informatico, la Direzione del Servizio Rapporti Istituzionali di Vigilanza e la Direzione del Dipartimento di Vigilanza Bancaria e Finanziaria.

Indirizzo
Via Nazionale 91
00184 Roma - Italia

Sito internet
http://www.bancaditalia.it

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia

INDICE

1. Introduzione 5

2. Evidenze 6

2.1 Le cause degli incidenti 7

Gli incidenti operativi 7

Gli incidenti cyber 8

Coinvolgimento dei fornitori di servizi 9

2.2 Gli impatti degli incidenti e le tempistiche di risoluzione 9

3. Conclusioni 12

1. Introduzione

Il presente report sintetizza le principali evidenze provenienti dalle segnalazioni dei "gravi incidenti operativi o di sicurezza"[1] notificati nell'anno 2024 dagli intermediari alla Banca d'Italia in base alle previsioni della Circolare n.285, alle Disposizioni di vigilanza per gli istituti di pagamento (IP) e gli istituti di moneta elettronica (IMEL) e alle istruzioni operative rese disponibili sul sito internet dell'Istituto[2]. Le segnalazioni vengono raccolte nell'ambito di un *framework* di gestione degli incidenti a cura del Dipartimento di Vigilanza Bancaria e Finanziaria[3].

Nel 2024 sono state trasmesse alla Banca d'Italia 188 segnalazioni di gravi incidenti operativi o di sicurezza, in significativo aumento rispetto a quelle ricevute nel 2023 (circa il 45% in più). I principali trend riguardano l'aumento generale delle segnalazioni nel periodo considerato, con una prevalenza di incidenti operativi (79% del totale), il forte coinvolgimento dei fornitori di servizi esterni nelle segnalazioni (65% del totale) e una leggera crescita del numero di incidenti *cyber* (+8%)[4]. Per questi ultimi, sono in diminuzione gli attacchi di tipo *Distributed Denial of Service* (DDoS), che nel 2023 rappresentavano la tipologia prevalente. Gli impatti economici degli incidenti continuano ad essere limitati seppur in aumento rispetto agli anni precedenti; in pochi casi, tuttavia, gli impatti superano i € 2 mln. È in aumento anche l'impatto sulla disponibilità dei servizi, in termini di tempo necessario per il ripristino degli stessi.

Nel seguito del documento, il Capitolo 2 fornisce i principali *trend* osservati nel 2024, con un approfondimento su cause (paragrafo 2.1), impatti e tempistiche di risoluzione (paragrafo 2.2), mentre il Capitolo 3 riporta le principali conclusioni.

---

1 La normativa definisce incidente operativo o di sicurezza "ogni evento, o serie di eventi collegati, non pianificati dalla banca che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, e/o l'autenticità dei servizi".

2 Il *framework* si applica a banche (incluse succursali di banche extracomunitarie), IP e IMEL.

3 Il 2024 rappresenta l'ultimo anno in cui è stato in vigore il quadro di segnalazione dei gravi incidenti operativi o di sicurezza sopra citato; a decorrere dal 17/01/2025, infatti, esso è stato aggiornato per essere allineato al regolamento UE 2022/2554 (*Digital Operational Resilience Act* - DORA), come richiamato dalla comunicazione della Banca d'Italia del 27 dicembre 2024 (per maggiori dettagli, cfr. sul sito della Banca d'Italia: Comunicazione di gravi incidenti ICT e delle minacce informatiche significative https://www.bancaditalia.it/compiti/vigilanza/dora-incidenti/index.html). Il *framework* DORA si muove comunque in continuità con quello precedente, estendendo l'obbligo segnaletico a nuove entità finanziarie (ad esempio imprese di investimento, gestori, emittenti di *token* collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di *crowdfunding*) e introducendo un nuovo tipo di segnalazione, su base volontaria, delle minacce informatiche significative.

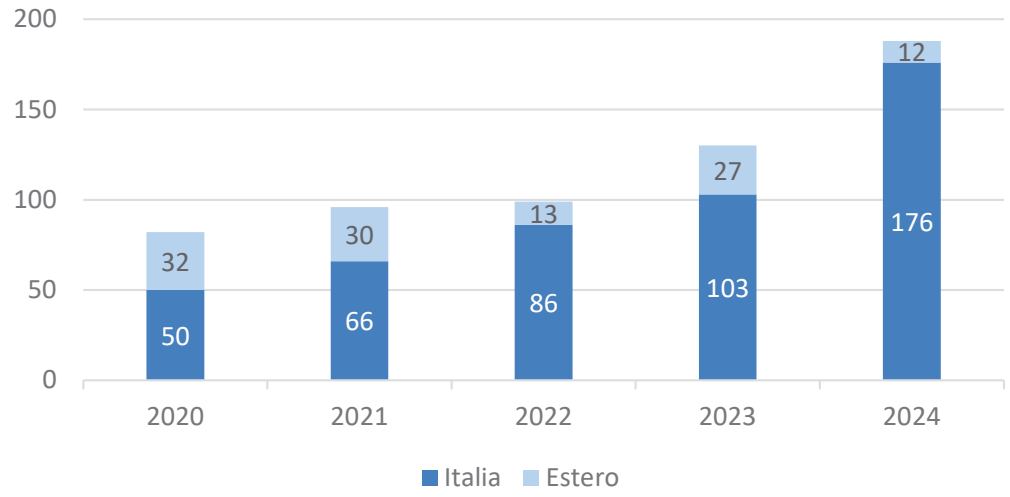
4 Si confermano quindi i principali trend delineati, per il periodo 2020-23, nel documento di analisi pubblicato dalla Banca d'Italia "*Digital resilience in the Italian financial sector: evidences from the supervisory incident reporting framework*" (https://www.bancaditalia.it/media/notizia/digital-resilience-in-the-italian-financial-sector-documento-di-analisi-della-banca-d-italia/).

2. Evidenze

Il numero di segnalazioni di gravi incidenti operativi o di sicurezza ricevute nel 2024 è in significativa crescita rispetto agli anni precedenti (188 contro le 130 del 2023 e le 99 del 2022 – cfr. Figura 1)[5]. Il numero di singoli eventi segnalati[6] (103) è in lieve diminuzione rispetto al 2023 (113), indice del fatto che i singoli eventi hanno coinvolto, in media, più intermediari.

Figura 1

SEGNALAZIONI INCIDENTI PER GIURISDIZIONE INTERESSATA (1)



(1) Il totale delle segnalazioni comprende quelle delle controllate estere dei gruppi italiani.

Le 188 notifiche ricevute sono riferibili a 73 intermediari distinti, pari al 47% del totale degli intermediari vigilati nel perimetro del *framework*. Il numero di soggetti segnalanti risulta in significativa crescita[7]; tuttavia, si rileva che 29 intermediari (circa il 40%) hanno segnalato un solo incidente nel corso dell'anno.

Tra gli incidenti segnalati nel 2024, quelli operativi sono circa il 79% del totale (cfr. Figura 2), in deciso aumento rispetto al 2023 (148 rispetto a 93, +59%). Gli incidenti *cyber* segnalati nel 2024 – circa il 21% del totale delle segnalazioni – sono in leggero aumento rispetto all'anno precedente (40 rispetto a 37, +8%). Come nel 2023 gli incidenti *cyber* sono principalmente segnalati dalle banche *significant*, rispetto a banche *less significant* e altri operatori (cfr. Figura 3).

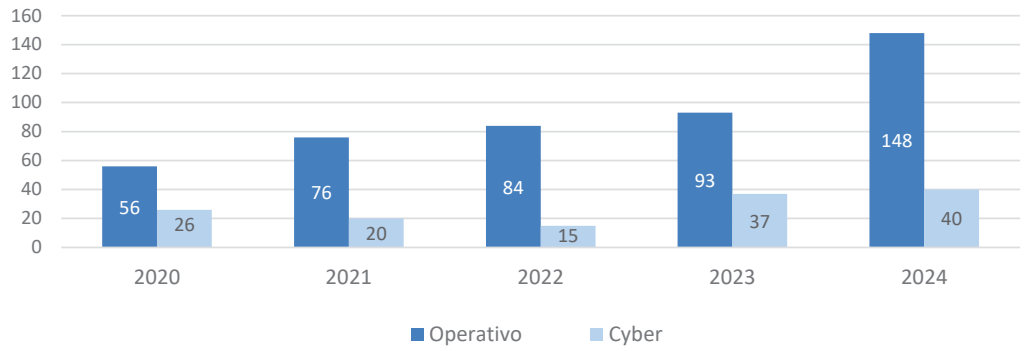
5 Dopo un incremento del numero di segnalazioni di incidenti con impatti sulle controllate estere di gruppi italiani avvenuto nel 2023, si rileva un nuovo decremento di tali casistiche nel 2024.

6 Ovvero contando i singoli eventi che hanno fatto scaturire diverse segnalazioni.

7 La percentuale di segnalanti era stata 12% nel 2020, 19% nel 2021, 29% nel 2022, 26% nel 2023.

Figura 2

SEGNALAZIONI INCIDENTI PER CLASSIFICAZIONE (OPERATIVO VS *CYBER*)

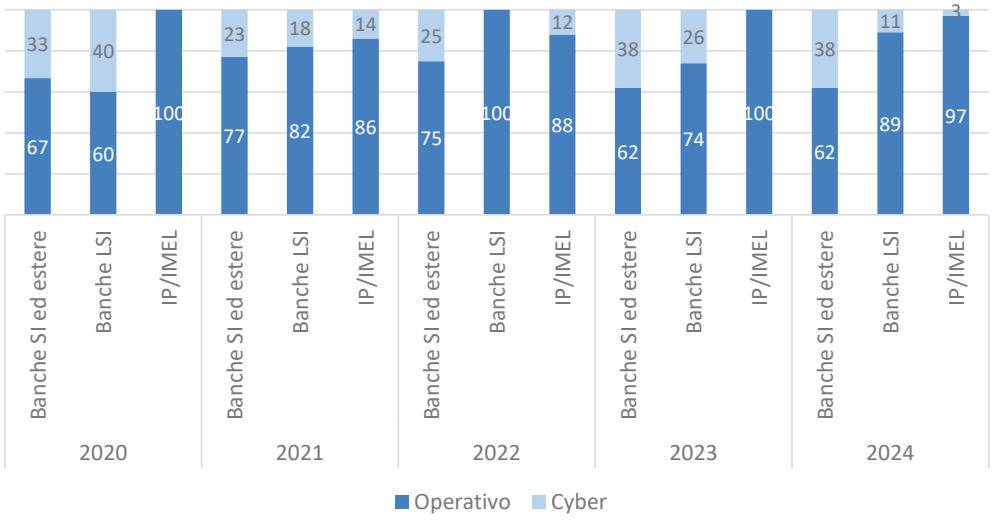


% / Anno	2020	2021	2022	2023	2024
Operativo	68%	79%	85%	72%	79%
Cyber	32%	21%	15%	28%	21%

Figura 3

CLASSIFICAZIONE INCIDENTI (OPERATIVI VS *CYBER*) PER CATEGORIA DI INTERMEDIARI

(valori percentuali)



2.1 Le cause degli incidenti

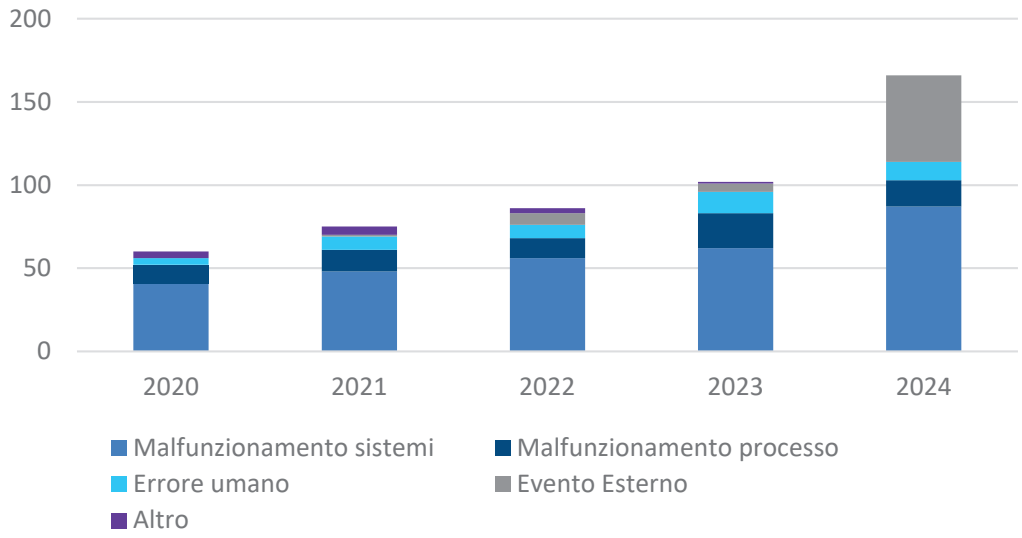
Gli incidenti operativi

Per gli incidenti operativi, in linea con gli anni passati, la causa principale è rappresentata da malfunzionamenti, legati principalmente a problemi *software,* e in parte minoritaria a problemi *hardware*; seguono poi errori umani ed errori dovuti

a processi (cfr. Figura 4). Gli incidenti operativi dovuti ai cambiamenti (cd. *IT changes*) hanno rappresentato circa il 30% del totale degli incidenti operativi.

Figura 4

SEGNALAZIONI INCIDENTI OPERATIVI PER TIPOLOGIA

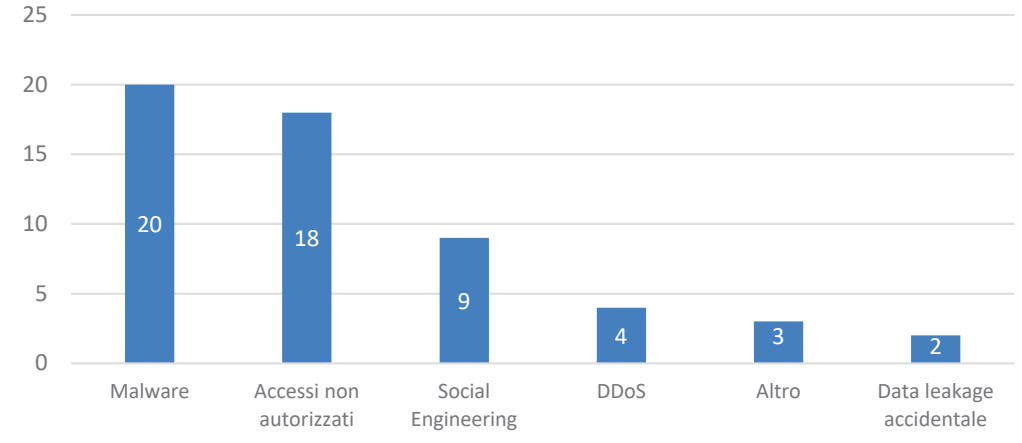


Gli incidenti cyber

Le 40 segnalazioni di incidenti cyber pervenute alla Banca d'Italia nel 2024 (contro le 37 del 2023, +8%) sono scaturite da 30 distinti eventi, riferibili a 28 attacchi informatici e 2 *data leakage* accidentali. Nel 2024 si evidenzia una importante diminuzione degli attacchi di tipo DDoS rispetto all'anno precedente (dai 16 del 2023 ai 4 del 2024, -75%), mentre aumentano tutte le altre tipologie di attacchi, tra cui gli attacchi di tipo *malware*, comprendenti anche i *ransomware*, gli attacchi condotti tramite accesso non autorizzato e gli attacchi di *social engineering* (cfr. Figura 5).

Figura 5

SEGNALAZIONI INCIDENTI CYBER PER TIPOLOGIA – ANNO 2024



Nel corso dell'anno l'Istituto ha effettuato un'analisi di dettaglio sugli incidenti *cyber* segnalati dagli intermediari tra gennaio 2023 e maggio 2024. Dagli approfondimenti è emerso come la maggior parte degli attacchi *cyber* sia riconducibile a *threat actor* noti e che in alcuni casi gli attacchi informatici abbiano provocato impatti economici non trascurabili, in particolare a seguito di attacchi *malware* e di *social engineering* che hanno colpito gli intermediari direttamente.

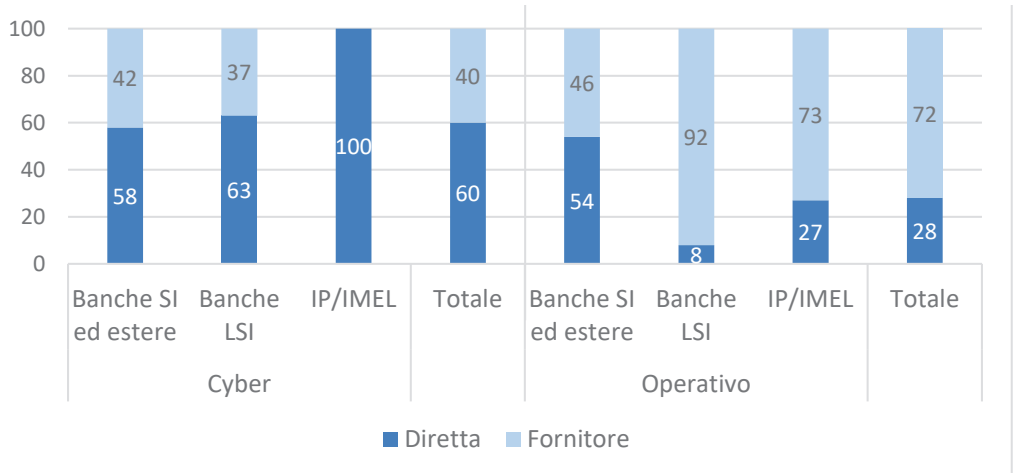
Coinvolgimento dei fornitori di servizi

Nel 65% degli incidenti segnalati è coinvolto un fornitore di servizi, in misura maggiore per gli incidenti operativi rispetto a quelli *cyber*; il dato risulta in aumento rispetto al 2023 (circa 45%). Il fornitore è all'origine dell'incidente nella maggior parte degli incidenti operativi per le banche *less significant* e per gli IP e IMEL (cfr. Figura 6).

Figura 6

RESPONSABILITÀ PER CLASSIFICAZIONE E CATEGORIA DI INTERMEDIARI – ANNO 2024

(valori percentuali)



L'elevato numero di incidenti che coinvolgono un fornitore di servizi conferma come l'interconnessione tra i vari soggetti nel mercato rappresenti un rischio per gli intermediari, data la possibilità che problemi sulle terze parti esterne al perimetro di supervisione si ripercuotano sui soggetti vigilati.

2.2 Gli impatti degli incidenti e le tempistiche di risoluzione

Anche nel 2024 la maggior parte degli incidenti (circa l'80%) ha interessato i servizi di pagamento (ATM[8], *web* e *mobile banking*, pagamenti all'ingrosso, ecc.), con una percentuale in linea con gli anni precedenti (cfr. Figura 7). I servizi di pagamento continuano ad essere principalmente affetti da incidenti operativi (cfr. Figura 8).

8 *Automated Teller Machine.*

Figura 7

SEGNALAZIONI CON IMPATTO SUI SERVIZI DI PAGAMENTO
(valori percentuali)

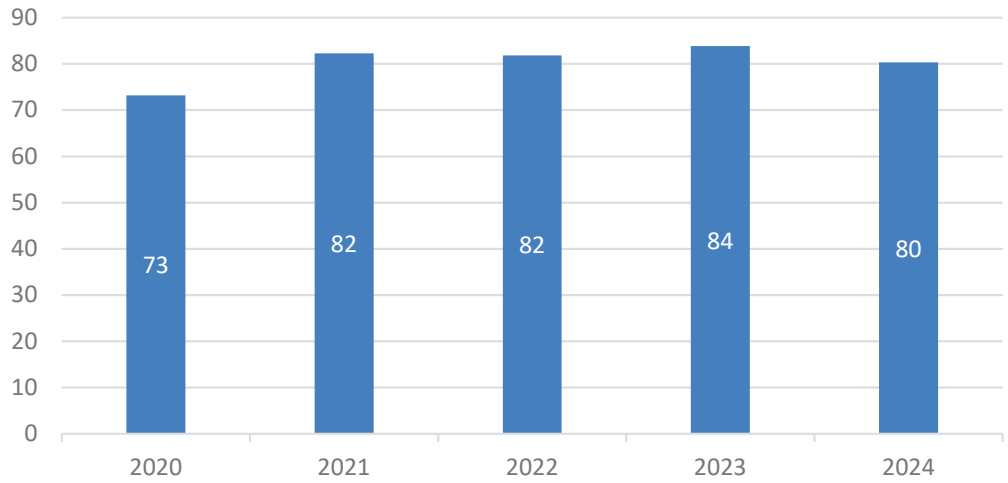
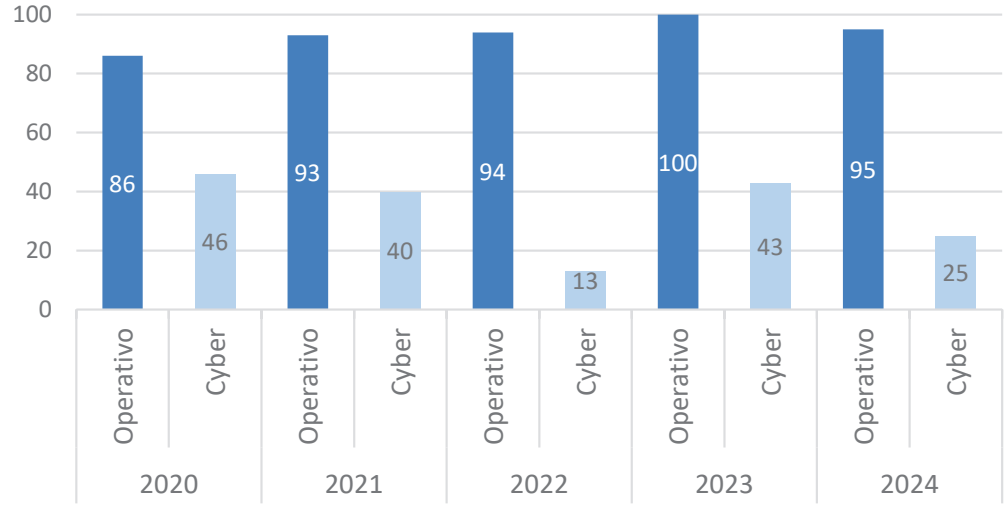


Figura 8

SEGNALAZIONI CON IMPATTO SUI SERVIZI DI PAGAMENTO PER CLASSIFICAZIONE
(valori percentuali)



L'interruzione della disponibilità e della continuità dei servizi rappresenta la principale conseguenza degli incidenti e caratterizza tutte le tipologie di intermediari. Complessivamente circa il 70% degli incidenti totali ha comportato l'interruzione di un servizio (sia esso di pagamento, *core banking* o ad essi ancillare). In particolare, tali incidenti hanno prodotto mediamente circa 21 ore di interruzione dei servizi, un dato in deciso aumento rispetto alle 9 ore del 2023, principalmente a causa di eventi operativi relativi a fornitori. Allo stesso tempo, gli incidenti che hanno impatti su servizi

rilevanti[9] e su un significativo numero di clienti[10] (il 22% del totale dei 188 incidenti segnalati) presentano un tempo medio di ripristino mediamente minore (circa 13 ore), seppur in aumento rispetto al 2023 (circa 5 ore).

Gli impatti economici degli incidenti sono, nella maggior parte dei casi, non rilevanti. Tuttavia in pochi casi (7 su 188) si rileva un impatto economico[11] sull'intermediario superiore a € 2 mln, in particolare a seguito di attacchi di *social engineering* diretti verso gli organi apicali degli intermediari, di attacchi *malware* diretti ai sistemi degli intermediari, di *IT change* errati o di errori operativi.

9 Sono ritenuti rilevanti i servizi *time sensitive*, ad esempio online banking, ATM, ecc.

10 i.e. potenzialmente oltre 100.000 clienti.

11 Nell'ambito del *framework* di segnalazione incidenti, per impatto economico si intende l'intero ammontare delle perdite sia dirette che indirette espresso in euro. Tra i costi da annoverare ci sono, a puro titolo esemplificativo, costi di sostituzione *hardware* e/o *software*, sanzioni per il mancato rispetto di obblighi contrattuali, mancati ricavi, ecc. Nelle fasi immediatamente successive alla rilevazione dell'incidente quantificare esattamente le perdite economiche risulta spesso complicato e pertanto l'intermediario comunica delle stime di massima. Nell'ambito dei successivi previsti aggiornamenti dell'incidente, tali stime vengono via via perfezionate, ma in alcuni casi l'effettiva reale quantificazione avviene molto tempo dopo la chiusura dell'incidente o può anche non avvenire (ad esempio in relazione a potenziali spese legali, mancati ricavi dovuti alla perdita di opportunità commerciali, ecc.).

3. Conclusioni

Il *framework* di segnalazione degli incidenti operativi o di sicurezza si conferma come uno degli strumenti di vigilanza più efficaci per il monitoraggio e l'analisi del rischio operativo degli intermediari vigilati e dei fornitori. Esso rappresenta un valido strumento per la valutazione tempestiva dei *trend* di sistema rispetto a nuove minacce e vulnerabilità comuni al mercato finanziario italiano.

Le evidenze raccolte nel 2024 mostrano che:

- il numero totale di incidenti segnalati nel 2024 è in deciso aumento rispetto all'anno precedente (+45%), sebbene il numero di singoli eventi a cui questi si riferiscono risulta in diminuzione (-9%), indice del fatto che i singoli eventi hanno coinvolto, in media, più intermediari;
- la gran parte delle segnalazioni riguarda incidenti operativi (79% del totale), sebbene gli incidenti *cyber* segnalati nel 2024 siano in leggero aumento rispetto all'anno precedente (+8%);
- nel 65% degli incidenti segnalati è coinvolto un fornitore di servizi (era circa il 45% nel 2023), in misura maggiore i) per gli incidenti operativi rispetto a quelli cyber (per cui rispettivamente il 72% e il 40% ha coinvolto un fornitore) e ii) per le banche *less significant* (86%), IP e IMEL (71%) rispetto alle banche *significant* (44%);
- in linea con gli anni passati, la causa principale di incidenti operativi è rappresentata da malfunzionamenti, principalmente legati a problemi *software*; inoltre, gli incidenti operativi dovuti ai cambiamenti (cd. *IT changes*) hanno rappresentato circa il 30% del totale;
- riguardo gli incidenti *cyber* si evidenzia una diminuzione degli attacchi di tipo DDoS rispetto all'anno precedente, mentre aumentano tutte le altre tipologie di attacchi, tra cui gli attacchi di tipo *malware*, che comprendono anche i *ransomware*, gli attacchi condotti tramite accesso non autorizzato e gli attacchi di *social engineering*;
- gli incidenti che hanno impatti sulla disponibilità dei servizi rilevanti e su un significativo numero di clienti rappresentano il 22% del totale e risultano collegati prevalentemente a incidenti operativi occorsi presso fornitori di servizi;
- anche gli impatti economici degli incidenti sono di norma non rilevanti; tuttavia, 7 segnalazioni hanno riportato un impatto economico superiore a € 2 mln.

I principali rischi evidenziati nelle analisi qui riportate vengono confermati anche dagli studi dell'Agenzia Europea per la Cybersicurezza (ENISA)[12] e dalla BCE[13],

12 Cfr. ENISA, *Threat Landscape* 2024.

13 Cfr. ECB, *Evolving IT and cybersecurity risks*, novembre 2024.

che indicano gli attacchi *ransomware* come una delle principali minacce a livello europeo, anche per il settore bancario. Al contempo, la compromissione delle mail aziendali tramite attacchi di *social engineering* risulta una delle principali tecniche di frode segnalate secondo gli studi dell'EUROPOL[14]. Tra le principali differenze, invece, emerge che gli attacchi DDoS rimangono numerosi a livello europeo, mentre i dati provenienti dalle segnalazioni ne evidenziano una diminuzione.

Il 2024 rappresenta l'ultimo anno in cui le segnalazioni sono state effettuate tramite il *framework* di segnalazione degli incidenti della Banca d'Italia, in quanto – dal 17 gennaio 2025 – è entrato in vigore il nuovo schema di segnalazione legato al regolamento DORA, che il nostro Istituto ha reso immediatamente operativo. La segnalazione degli incidenti è uno dei pilastri principali del regolamento, che prevede l'obbligo segnaletico quasi in tempo reale e il rafforzamento dei processi di coordinamento tra Autorità europee e nazionali, ad esempio tramite la trasmissione immediata delle segnalazioni ricevute dalle *banche significant* alla BCE o la condivisione delle informazioni degli incidenti segnalati in uno Stato membro con impatti in altri Stati. Il nostro Istituto ha iniziato a ricevere le prime segnalazioni di incidenti avvenuti in altri Paesi europei con potenziale impatto in Italia, le prime segnalazioni da parte di nuovi soggetti precedentemente esclusi dal *framework* e le prime notifiche volontarie di minacce informatiche significative da parte degli operatori di mercato. Questi elementi daranno la possibilità di migliorare le analisi di vigilanza sia a livello microprudenziale che macroprudenziale, permettendo di evidenziare i rischi legati alle tecnologie innovative che le diverse categorie di intermediari affrontano.

14 Cfr. EUROPOL, *Internet Organised Crime Threat Assessment* 2024.