BANCA D'ITALIA
EUROSISTEMA

Quadro segnaletico di Vigilanza dei gravi incidenti ICT

Analisi orizzontale 2025

Luglio 2026

BANCA D'ITALIA
EUROSISTEMA

Quadro segnaletico di Vigilanza dei gravi incidenti ICT

Analisi orizzontale 2025

Luglio 2026

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

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. Principali risultati **5**

2. Tipologie degli eventi **8**

Gli eventi operativi **8**

Gli eventi relativi alla cybersicurezza **8**

Coinvolgimento dei fornitori di servizi **9**

3. Gli impatti degli incidenti e le tempistiche di risoluzione **10**

4. Le minacce informatiche significative **11**

5. Confronto con lo schema segnaletico antecedente a DORA **11**

1. Principali risultati

Il Regolamento DORA - *Digital Operational Resilience Act* rappresenta il principale riferimento normativo per il rafforzamento della resilienza digitale nel sistema finanziario europeo. In tale contesto, la segnalazione dei gravi incidenti ICT costituisce un elemento fondamentale per monitorare il profilo di rischio informatico del sistema finanziario[1].

Il presente rapporto sintetizza le evidenze raccolte a livello nazionale tramite lo schema di segnalazione istituito dal Dipartimento di Vigilanza, in linea con le previsioni del regolamento DORA[2]. In particolare:

- Nel corso del 2025, 101 singoli eventi hanno dato luogo a 137 segnalazioni, inviate perlopiù da banche e gruppi bancari (cfr. Figura 1); rispetto al 2024 si osserva una diminuzione del numero complessivo delle segnalazioni a fronte di un aumento degli eventi[3].
- La maggior parte degli incidenti è di natura operativa (cfr. Figura 2) ed è prevalentemente associata a malfunzionamenti dei sistemi, in particolare di tipo *software*, seguiti da problemi di rete; circa il 30% degli eventi è inoltre riconducibile a cambiamenti nei sistemi ICT.
- Gli eventi relativi alla cybersicurezza rappresentano il 23% del totale e riguardano soprattutto casi di esfiltrazione di dati[4], seguiti da attacchi alla

1 Il regolamento DORA ha introdotto un nuovo quadro di segnalazione dei gravi incidenti ICT armonizzato a livello europeo, ampliando significativamente il perimetro dei soggetti obbligati alla segnalazione e aggiornando soglie e criteri di classificazione, pur in continuità con i precedenti quadri di segnalazione. Il nuovo quadro prevede inoltre la possibilità per i soggetti finanziari di notificare all'Autorità competente, su base volontaria, minacce informatiche significative, ovvero di trasmettere informazioni su minacce ritenute rilevanti per il sistema finanziario, per gli utenti dei servizi o per la clientela. Il regolamento ha inoltre previsto la possibilità per l'Autorità di richiedere annualmente alle entità vigilate una stima dei costi e delle perdite derivanti dai gravi incidenti ICT. La disponibilità di tali informazioni consentirà una valutazione più accurata degli impatti economici degli incidenti nel tempo, anche tenendo conto di eventuali recuperi, migliorando la qualità dello scambio informativo tra intermediari e Autorità di vigilanza.

2 Lo schema di segnalazione si applica ai seguenti soggetti vigilati: banche, imprese di investimento, gestori, istituti di pagamento, istituti di moneta elettronica, emittenti di token collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di crowdfunding, Cassa Depositi e Prestiti S.p.A. e Poste Italiane S.p.A., per l'attività di Bancoposta.

3 Lo schema di segnalazione dei gravi incidenti ICT previsto dal regolamento DORA richiede che le segnalazioni siano trasmesse all'Autorità di vigilanza dai singoli intermediari. In tale contesto, il termine evento indica il singolo accadimento che ha originato una o più segnalazioni, ad esempio un incidente riconducibile a un fornitore di servizi con impatti su più intermediari o gruppi. Nell'ipotesi che un evento coinvolga più intermediari appartenenti ad un medesimo gruppo bancario o di società di intermediazione mobiliare (SIM) sono attese tante segnalazioni quanti sono gli intermediari effettivamente coinvolti. Nel presente rapporto, salva diversa indicazione, le segnalazioni relative a un singolo evento inviate da più intermediari finanziari appartenenti al medesimo gruppo sono trattate come un'unica segnalazione.

4 L'esfiltrazione di dati è il trasferimento non autorizzato di informazioni da un sistema o rete verso un'entità esterna spesso utilizzando tecniche di compressione o cifratura per evitarne il rilevamento.

catena di fornitura[5] e da attacchi *ransomware*[6], mentre risultano marginali i casi di furti d'identità[7] e gli attacchi DDoS[8].

- In oltre la metà delle segnalazioni è coinvolto un fornitore o subfornitore di servizi. Il ruolo delle terze parti si conferma centrale nella gestione del rischio ICT; il rafforzamento delle misure di governance e di controllo del rischio di terza parte da parte degli intermediari è cruciale.
- Sotto il profilo degli impatti, l'interruzione dei servizi continua a costituire la conseguenza più frequente, interessando la maggior parte delle segnalazioni (70% del totale), mentre le perdite economiche risultano nel complesso contenute e concentrate in un numero limitato di casi di maggiore severità.

Nel complesso, le evidenze emerse risultano coerenti con le principali analisi disponibili a livello nazionale[9], europeo[10] e internazionale[11], che segnalano la rilevanza delle minacce informatiche, in particolare quelle orientate all'esfiltrazione dei dati e alla catena di fornitura.

È importante rafforzare la qualità delle segnalazioni e garantire un processo segnaletico efficace; ciò potrà contribuire a una migliore comprensione dell'esposizione agli incidenti ICT e delle connesse aree di vulnerabilità e di rischio.

Il dialogo continuo tra Autorità e intermediari rimane un fattore chiave per affrontare le sfide poste dalla crescente digitalizzazione. In tale prospettiva, la Banca d'Italia continuerà a promuovere un confronto costruttivo con i soggetti vigilati, volto a favorire una maggiore consapevolezza dei rischi ICT e a rafforzare l'efficacia complessiva dell'azione di vigilanza.

---

5 Un attacco alla catena di fornitura compromette componenti, fornitori o processi a monte con l'obiettivo di penetrare nell'obiettivo finale e stabilire un canale persistente per poter effettuare ulteriori azioni malevole.

6 *Software* malevolo finalizzato a inibire l'accesso al dispositivo colpito o ai dati in esso contenuti, anche mediante tecniche di crittografia. Tipicamente questa tipologia di programmi è in grado di propagarsi velocemente sulla rete telematica della vittima, rendendo indisponibili in poco tempo un elevato numero di sistemi. Tale azione è finalizzata a ottenere dalla vittima il pagamento di un riscatto, tipicamente in criptovaluta, per rendere nuovamente utilizzabili i sistemi infettati o i dati cifrati.

7 Tipologia di attacco in cui un attore malevolo ottiene e utilizza illecitamente le credenziali o i dati di identità digitale di un'altra persona (come *username*, *password*, *token*, attributi digitali o altri identificatori *online*) per compiere azioni fraudolente o ingannevoli nei suoi confronti.

8 Il termine DoS - *Denial of Service* (in italiano letteralmente negazione del servizio) nel campo della sicurezza informatica indica un attacco che impedisce l'accesso (autorizzato) alle informazioni e ai sistemi informativi o che determina un ritardo nell'esecuzione delle operazioni e funzioni dei sistemi informativi stessi, con il risultato di perdita della disponibilità per gli utenti autorizzati. Gli attacchi *denial-of-service* distribuito (attacco DDoS - *Distributed Denial of Service*) sono attacchi DoS portati avanti utilizzando diverse sorgenti contemporaneamente.

9 Agenzia per la Cybersicurezza Nazionale, *Operational Summary*, dicembre 2025.

10 ENISA, *Threat Landscape 2025*, ottobre 2025.

11 International Monetary Fund, *Good Practices in Cyber Risk Regulation and Supervision*, gennaio 2026.

Figura 1

NUMERO DI SEGNALAZIONI ED EVENTI

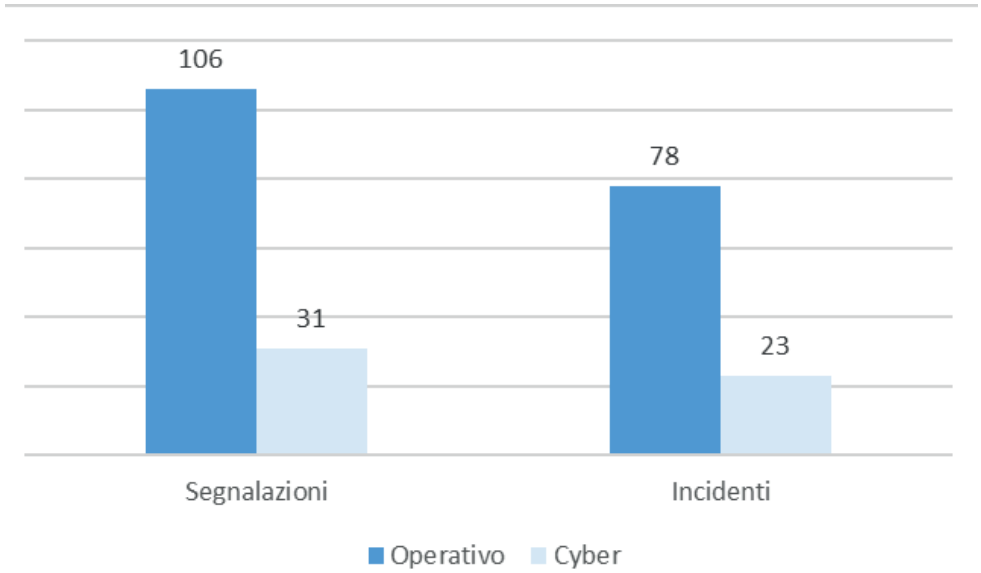
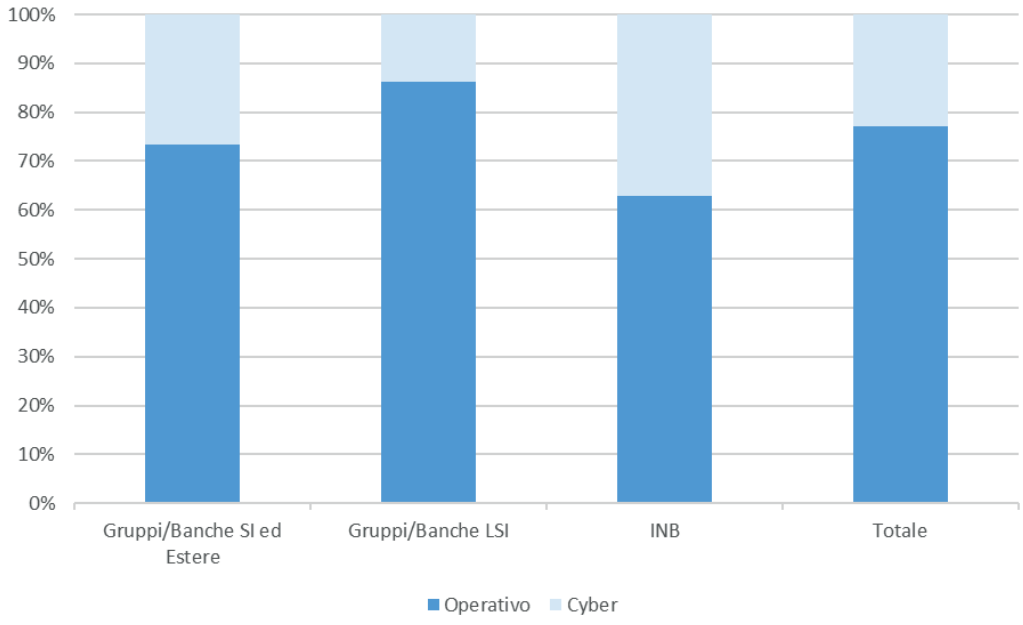


Figura 2

CLASSIFICAZIONE SEGNALAZIONI PER CATEGORIA DI INTERMEDIARI



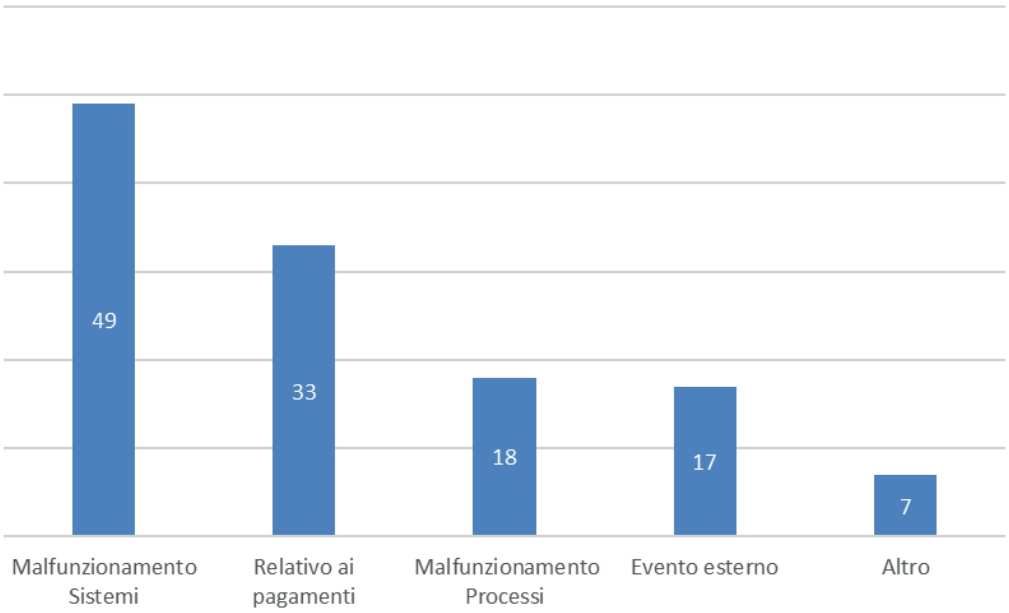
2. Tipologie degli eventi

Gli eventi operativi

La principale tipologia di eventi operativi segnalati è rappresentata da malfunzionamenti dei sistemi, legati principalmente a problemi *software*, e in parte minoritaria a problemi di rete (cfr. Figura 3). A questi seguono poi quelli relativi ai pagamenti[12], gli errori dovuti a processi e gli eventi esterni. Gli eventi operativi attribuibili ai cambiamenti dei sistemi ICT (cd. ICT *changes*) hanno rappresentato circa il 30% del totale.

Figura 3

EVENTI OPERATIVI PER TIPOLOGIA



Gli eventi relativi alla cybersicurezza

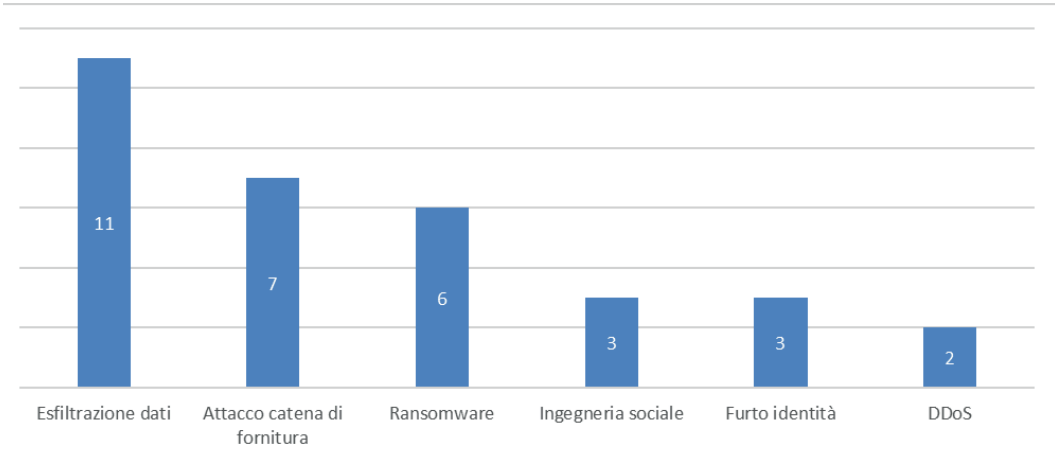
Nel corso del 2025, 23 singoli eventi relativi alla cybersicurezza hanno generato 31 segnalazioni. La maggior parte di questi sono riferibili a esfiltrazioni di dati, seguiti da attacchi alla catena di fornitura e attacchi *ransomware* (Figura 4); hanno una minore frequenza gli attacchi di ingegneria sociale[13], i furti d'identità e gli attacchi DDoS.

12 Si tratta di eventi che hanno interessato prioritariamente dati o servizi connessi ai pagamenti forniti dall'entità finanziaria.

13 Insieme di tecniche adottate dagli attaccanti informatici per manipolare psicologicamente e/o ingannare le vittime in modo da indurle a commettere azioni a proprio vantaggio nell'ambito di un'operazione di attacco cyber. Fanno parte di questa tipologia gli attacchi di *phishing*, ovvero attività illecite volte ad acquisire dati sensibili o riservati da soggetti.

Figura 4

EVENTI RELATIVI ALLA CYBERSICUREZZA PER TIPO DI ATTACCO

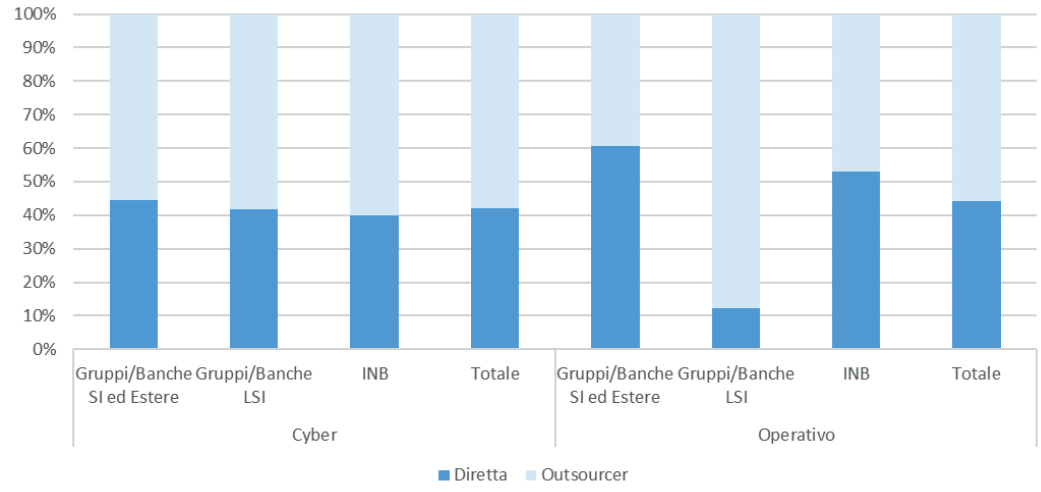


Coinvolgimento dei fornitori di servizi

Nel 56% delle segnalazioni risulta coinvolto un fornitore di servizi, con una proporzione sostanzialmente analoga tra segnalazioni operative e di cybersicurezza. Nel caso delle banche meno significative, il fornitore è all'origine dell'evento nella quasi totalità delle segnalazioni relative a incidenti operativi (cfr. Figura 5).

Figura 5

RESPONSABILITÀ PER CLASSIFICAZIONE E CATEGORIA DI INTERMEDIARI

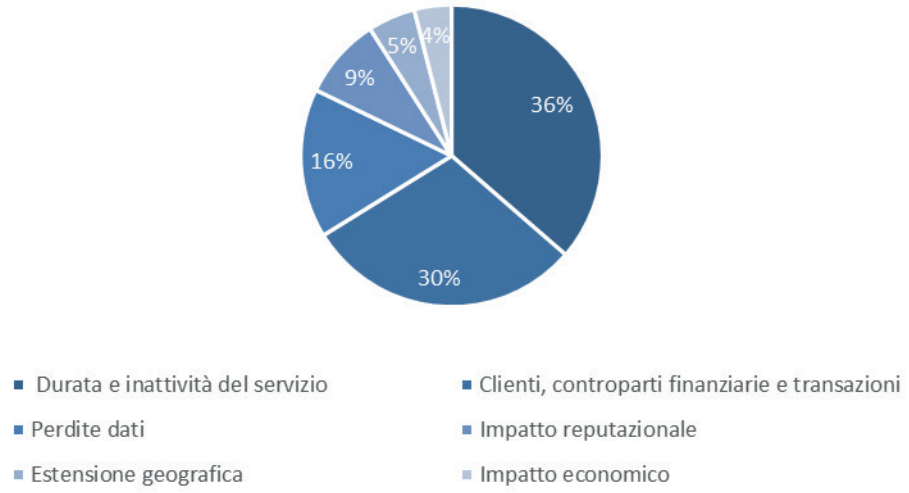


3. Gli impatti degli incidenti e le tempistiche di risoluzione

Il nuovo schema di segnalazione ha introdotto un aggiornamento dei criteri e delle soglie per la notifica dei gravi incidenti. Tra i criteri applicati, la durata dell'incidente e l'inattività del servizio risultano i più frequentemente indicati, seguiti da quelli relativi al numero di clienti, controparti finanziarie e transazioni impattate (cfr. Figura 6)[14]. Rilevante è inoltre l'incidenza delle perdite di dati, mentre risultano meno frequenti gli impatti reputazionali, geografici o economici.

Figura 6

CRITERI DI CLASSIFICAZIONE DELLE SEGNALAZIONI



Circa la metà delle segnalazioni indica una rilevazione immediata dell'evento; circa il 20% è stato individuato entro 8 ore e il 3% in un intervallo compreso tra le 8 e le 24 ore. Una porzione non trascurabile, pari a circa il 28%, è stata individuata dopo 24 ore: nella maggior parte dei casi si tratta di attacchi informatici o eventi operativi che non producono effetti immediati.

La principale conseguenza è l'inattività dei servizi: circa il 70% delle segnalazioni indica infatti l'interruzione di un servizio. Nella maggior parte dei casi, tali interruzioni hanno una durata non superiore alle 8 ore; in alcuni episodi si sono estese fino a 24 ore. Solo in un numero limitato di casi l'interruzione supera le 24 ore; si tratta prevalentemente di eventi originati presso terze parti e che hanno comportato un impatto economico irrilevante.

In circa 35% delle segnalazioni sono state riportate perdite economiche, seppur di bassa entità. Nei cinque episodi con perdite superiori a 1 milione di euro, il recupero è stato integrale solo in due casi, mentre negli altri è stato possibile un recupero parziale.

14 Le segnalazioni possono includere più criteri tra quelli previsti, in funzione delle soglie applicabili. Ai fini dell'analisi rappresentata in figura, i criteri segnalati dalle singole entità finanziarie sono stati aggregati, ottenendo pertanto i dati su base consolidata. Le percentuali riportate sono state calcolate come rapporto tra il numero di occorrenze di ciascun criterio e il totale dei criteri complessivamente segnalati su base consolidata.

4. Le minacce informatiche significative

Con riferimento alle minacce informatiche significative, nel corso del 2025 sono state ricevute 3 segnalazioni relative ad eventi che non si sono concretizzati in effettivi gravi incidenti per gli intermediari. In due casi, le segnalazioni hanno riguardato minacce ai dati degli intermediari, gestiti da fornitori terzi. Infine, una minaccia ha riguardato alcuni tentativi di accesso non autorizzato ai conti della clientela. Tali tentativi non hanno avuto esito, essendo stati in parte intercettati dai sistemi di sicurezza dell'intermediario e non essendo gli attori della minaccia in possesso del secondo fattore di autenticazione necessario per l'accesso ai conti.

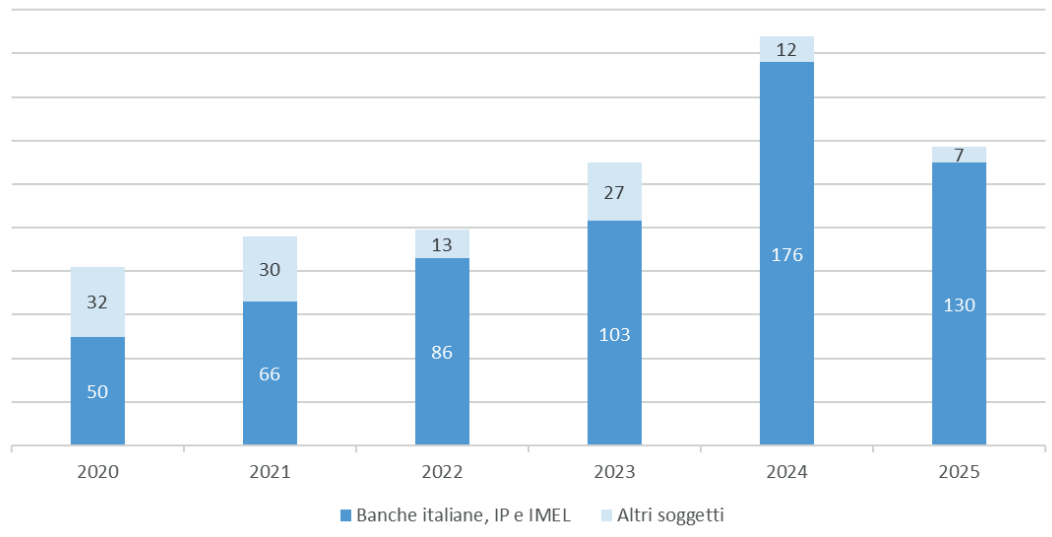
5. Confronto con lo schema segnaletico antecedente a DORA

L'entrata in vigore del regolamento DORA ha introdotto alcune discontinuità rispetto al preesistente modello segnaletico: oltre ad avere ampliato la platea delle entità finanziarie soggette all'obbligo di notifica, il regolamento ha infatti rivisto e aggiornato i criteri e le soglie per effettuare la segnalazione.

Facendo riferimento ai soli soggetti comuni ai due schemi segnaletici (banche italiane, istituti di pagamento e istituti di moneta elettronica), si osserva una riduzione del numero di segnalazioni nel corso del 2025 (cfr. Figura 7).

Figura 7

CONFRONTO CON LE SEGNALAZIONI ANTECEDENTI A DORA



Nonostante le segnalazioni risultino in calo rispetto all'anno precedente, il numero di singoli eventi occorsi nel 2025 risulta in crescita. In particolare, si registra un incremento degli eventi operativi, a fronte di una diminuzione degli eventi legati alla cybersicurezza (cfr. Figura 8). In linea con quanto osservato nel precedente schema, anche le segnalazioni

risultano prevalentemente riconducibili alla componente operativa in tutte le categorie di intermediari (cfr. Figura 9), sebbene nel 2025 si osservi un'incidenza maggiore della componente cyber per gli intermediari non bancari rispetto agli anni precedenti.

Figura 8

CONFRONTO CON GLI EVENTI ANTECEDENTI A DORA

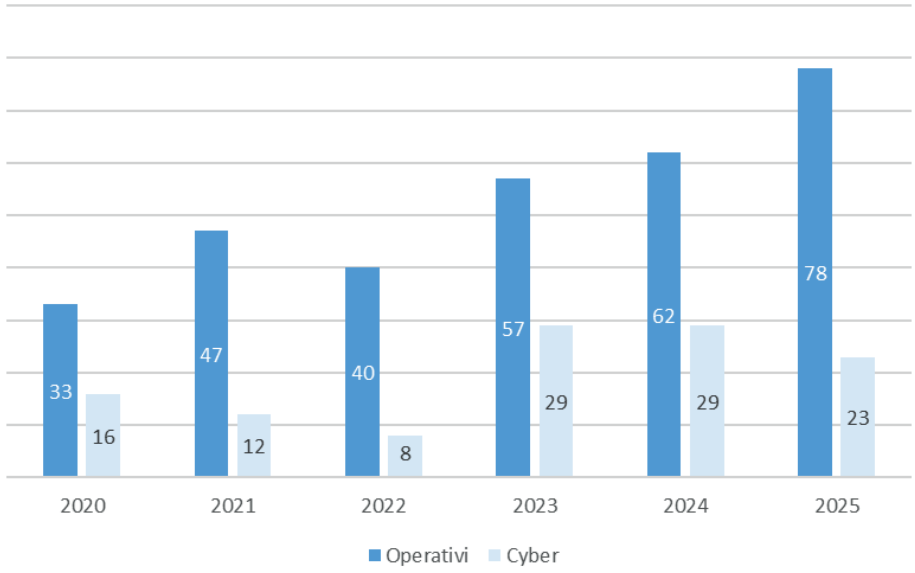
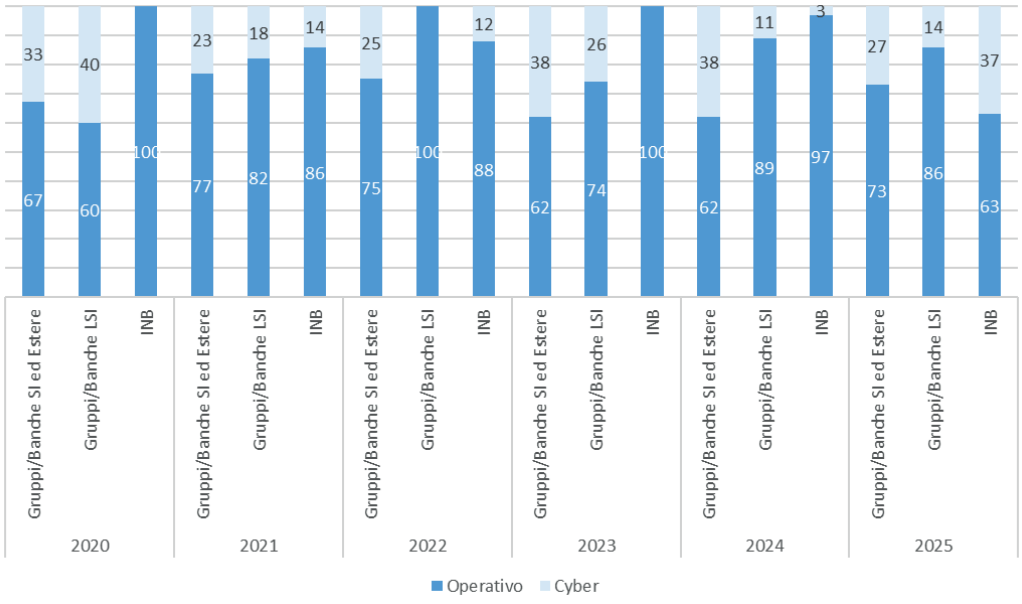


Figura 9

CLASSIFICAZIONE SEGNALAZIONI (OPERATIVE VS CYBER) PER CATEGORIA DI INTERMEDIARI [1]

(valori percentuali)



(1) Fino al 2024, in coerenza con il precedente schema segnaletico, tra gli intermediari non bancari sono ricompresi esclusivamente gli Istituti di pagamento (IP) e gli Istituti di moneta elettronica (IMEL) e, nelle segnalazioni relative ai gruppi SI, sono incluse anche quelle riferite alle controllate estere di gruppi SI italiani.

Rispetto al precedente schema, le cause degli eventi operativi restano sostanzialmente invariate: i malfunzionamenti dei sistemi continuano a rappresentare la principale causa e anche gli errori di processo si mantengono in linea con le precedenti evidenze. Gli eventi esterni mostrano invece una maggiore volatilità nel tempo. Anche gli incidenti riconducibili a cambiamenti ICT rimangono coerenti con quanto osservato nel vecchio schema segnaletico.

Per quanto riguarda gli eventi relativi alla cybersicurezza, l'utilizzo di *software* malevoli – intesi sia come *ransomware* sia come *software* finalizzato all'esfiltrazione dei dati – si conferma come la tecnica prevalentemente utilizzata. Gli attacchi di tipo DDoS si mantengono su livelli stabili, mentre quelli di ingegneria sociale risultano invece in diminuzione.

Il coinvolgimento dei fornitori di servizi ICT negli incidenti rimane elevato, pari a circa il 57% (cfr. Figura 10). Anche gli impatti si mantengono complessivamente in linea con il passato: l'interruzione della disponibilità e della continuità dei servizi continua a rappresentare la principale conseguenza. Si osserva però una diminuzione degli incidenti che hanno comportato perdite economiche rilevanti.

Figura 10

COINVOLGIMENTO DEI FORNITORI DI SERVIZI NELLE SEGNALAZIONI DI INCIDENTE