La copertura assicurativa nell’era di NIS2: dai trend degli attacchi alla gestione dei sinistri

Jacopo Gamba | WTW

Il crescente rischio informatico

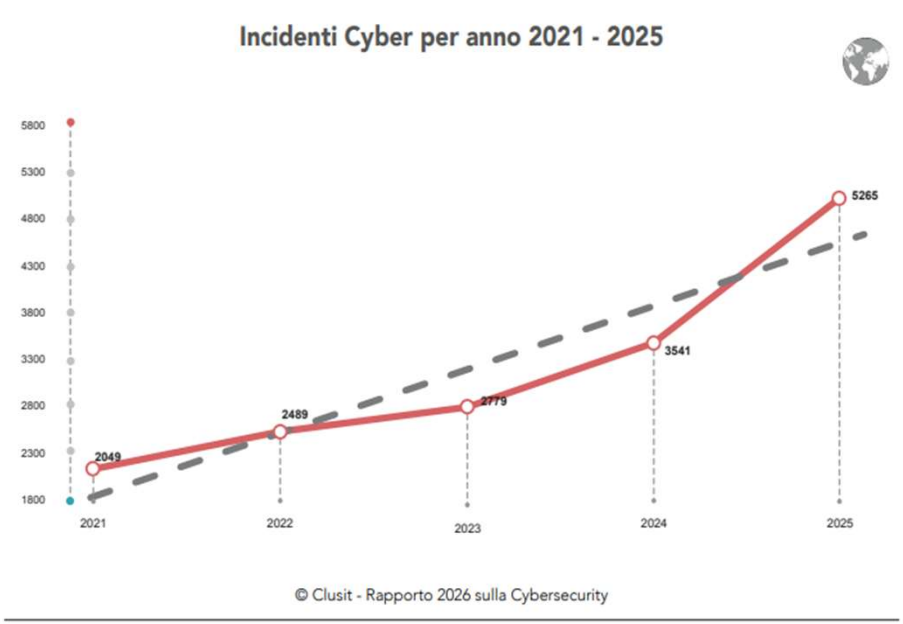


Fig. 1 - Andamento degli incidenti cyber nel periodo 2021 - 2025

*«(..) Nell'ultimo anno abbiamo registrato **5.265 incidenti**, quota che rappresenta non solo il **maggior numero registrato finora** in termini assoluti, ma anche un incredibile **aumento del 48,7% rispetto all'anno precedente**»*

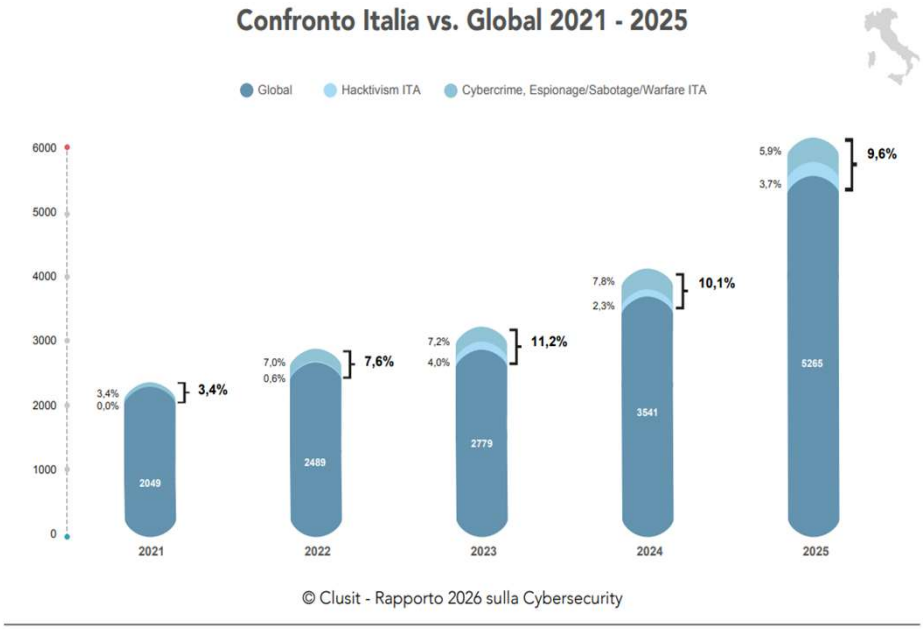


Fig. 26 - Incidenza degli incidenti in Italia rispetto al campione globale – 2021 - 2025

*«(..) nel 2025 il **dato italiano** rappresenta il **9,6%** del campione complessivo **degli incidenti individuati in tutto il mondo**.»*

Fonte: https://clusit.it/rapporto-clusit/

Il rischio informatico oggi come rischio di governance

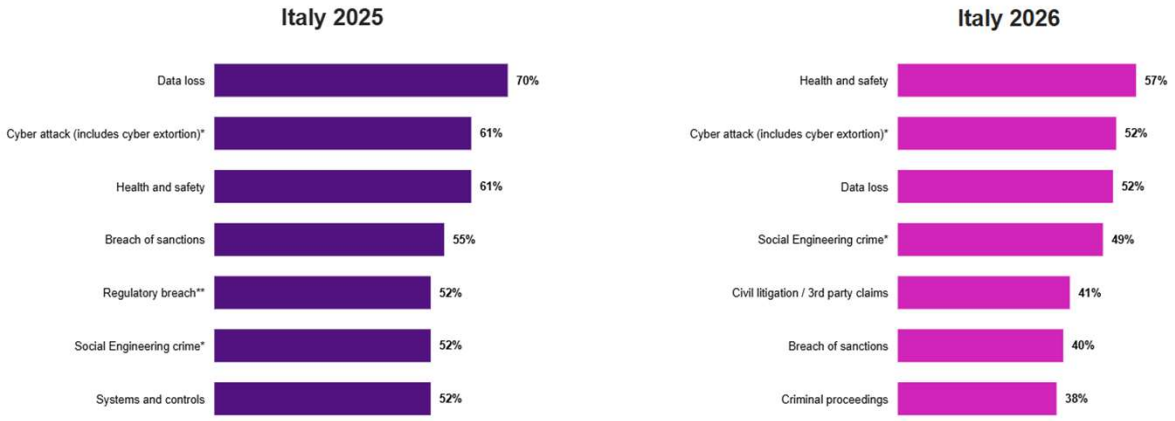
Con l'entrata in vigore di ***Dora*** (Regolamento Ue 2022/2554) e ***Nis 2*** (Direttiva Ue 2022/2555 recepita con dlgs 138/2024), senza dimenticare altre norme di settore quali ***Gdpr***, ***AI Act*** e ***Cyber resilience act***, il concetto di governance aziendale si amplia enormemente.

NIS 2

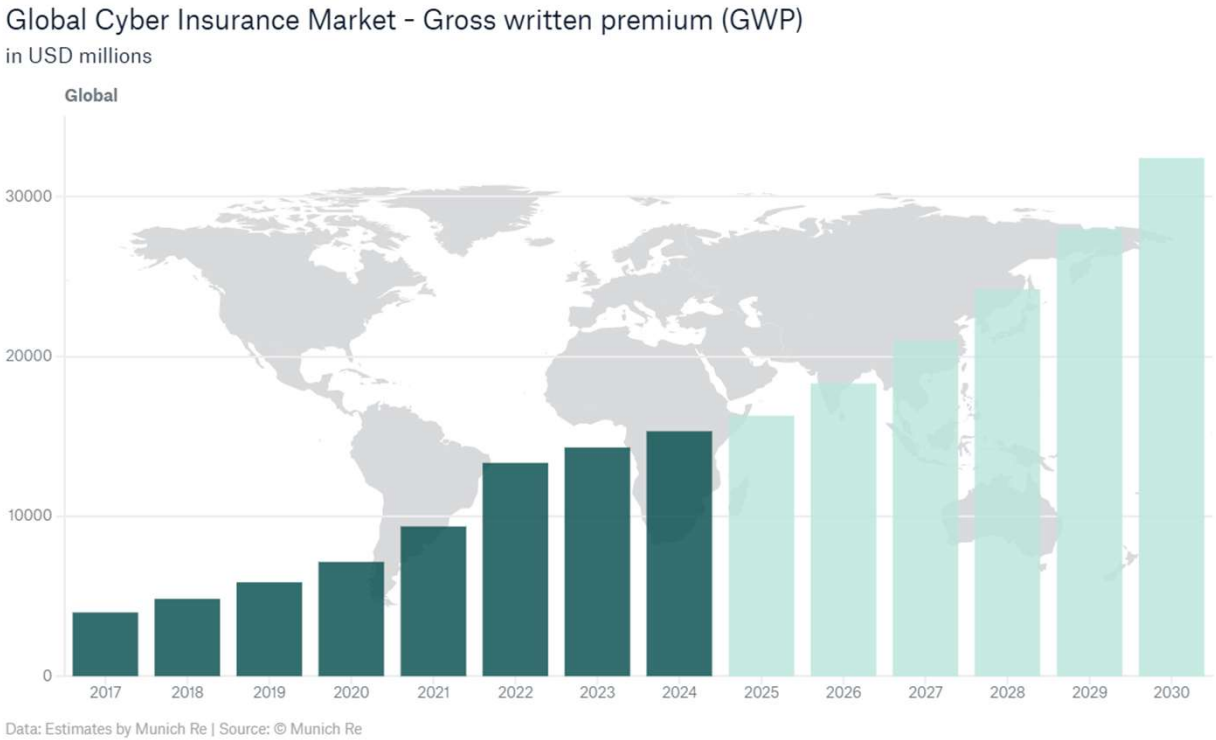
- ***Art. 20:*** gli organi di gestione approvano, supervisionano e rispondono delle misure di cybersecurity→ responsabilità diretta e personale degli amministratori
- ***Obbligo di competenze:*** il management deve ricevere formazione adeguata sul rischio cyber→ il difetto di competenza può integrare mancata diligenza
- ***Sanzioni e misure correttive:*** sanzioni fino a 10 M€ o 2% del fatturato globale→ possibili misure interdittive nei confronti del management

- ***Art. 2086, comma 2, c.c:*** obbligo degli amministratori di adottare assetti organizzativi, amministrativi e contabili adeguati→ oggi il cyber risk è pacificamente un rischio rilevante per la continuità aziendale
- ***Art. 2392 c.c. / 2476 c.c:*** responsabilità per mancata diligenza e omessa vigilanza→ l'ignoranza tecnica non è più contemplata, in presenza di un rischio noto e sistemico

Top 7 risks to Directors and Officers



La risposta del mercato assicurativo



Market Momentum	Scenari di rischio	Premi	Termini e condizioni
Soft Market – più capacità e più players	Ransomware - supply chain - rischio sistemico - AI	Decrescita, soprattutto per aziende con una ottima postura di sicurezza	Continuo ampliamento

Rischio cyber ed elementi assicurativi

La polizza assicurativa Cyber Risk consente di trasferire la perdita economica subita dalla società, derivante da

Violazione del sistema informatico assicurato da parte di terzi

Interruzione / malfunzionamento del sistema informatico

1. Spese di gestione dell'emergenza

Esempi:

- Costi di **informatica forense**;
- Spese di **assistenza legale**;
- Costi di **ripristino dei dati e dei sistemi**;
- **Costi di notifica** della violazione dei dati personali
- Spese per mitigare il **danno d'immagine**

2. Danni diretti

- **Perdita di profitto** per interruzione totale o parziale dei sistemi informatici, anche se dovuta ad incidente che ha colpito un fornitore esterno;
- **Costi operativi straordinari**;
- Spese per investigare e far fronte ad una **minaccia cyber di tipo estorsivo**;

3. Responsabilità civile verso terzi

Richieste di risarcimento da parte di terzi per:

- **Violazione di informazioni confidenziali**
- **Violazione della sicurezza** di terzi

Alcuni esempi di sinistro

Caso n. 1: Attacco Ransomware / Spese di Gestione della Crisi

- Azienda cliente subisce attacco tramite **ransomware "Conti"**.
- Nella notte l'antivirus mette in quarantena alcuni PC e viene verificata un'**infezione tramite *lateral movement*** (tecnica utilizzata dagli hacker per spostarsi progressivamente da un punto di ingresso compromesso al resto della rete, mentre cercano dati sensibili o altre risorse di alto valore da sottrarre).
- I PC ed i Server vengono messi immediatamente in quarantena e scollegati dalla rete precauzionalmente.
- A questo punto viene rilevato che alcune cartelle sono state criptate e viene inviata all'Assicurato una richiesta di riscatto: gli hacker sostengono di aver rubato **500 GB di informazioni**.
- Si rende così necessaria la **notifica all'autorità garante**, non sono italiana, ma anche di altri Paesi.
- L'azienda è costretta a sostenere **numerosi costi diretti**, dovendosi rivolgere a esperti esterni per affrontare la situazione.

Conti è una gruppo di hacker che utilizzano la tecnica del **Ransomware**, attivo dal 2020 in Russia.

Conti è particolarmente noto per l'utilizzo di tecniche Ransomware a **doppia estorsione**, in cui non solo i file delle vittime vengono criptati ma vi è anche una minaccia di pubblicazione degli stessi, in caso di mancato pagamento del riscatto.

In particolare, l'azienda sostiene costi per:

- Effettuare **analisi forensi**;
- Spese di **crisis management**;
- **Monitoraggio dei dati** sul web;
- Costi per **notifiche alle Autorità Garanti** di vari paesi;
- Spese per ingaggiare un **esperto negoziatore** per il dialogo con gli attaccanti;
- Costi di **ripristino dati**.

La richiesta di riscatto non ha avuto alcun seguito, non sono state ricevute richieste di risarcimento da terzi relative alla possibile diffusione dei dati e l'attacco non ha portato ad un'interruzione di attività rilevante.

Il danno è pertanto limitato ai costi diretti sostenuti per fronteggiare l'attacco.

L'assicuratore, tempestivamente informato degli incarichi attribuiti e costantemente aggiornato sulle attività svolte e sui costi maturati, ha riconosciuto in buona parte i costi sostenuti: quietanza di **€ 284.439,62 al netto della franchigia**.

Caso n. 2: Attacco di tipo “Distributed Denial-of-Service” (Ddos) / Perdite Proprie

L’attacco Ddos consiste nel **sovraccaricare un sito web, un server o una risorsa di rete con traffico dannoso**.

Di conseguenza, il sistema preso di mira si blocca o non riesce a funzionare, negando il servizio agli utenti legittimi e impedendo al traffico legittimo di arrivare a destinazione.

- L’azienda cliente subisce un **attacco di tipo Ddos** (Distributed Denial-of-Service).
- L’incidente si protrae per **più di 24 ore**, portando l’azienda a decidere di **bloccare alcuni sistemi con conseguente degrado dei canali di vendita**.
- Si rilevano **danni da perdita di profitto** (principalmente legati al calo dei ricavi provenienti dal canale mobile).
- **Non sono stati sostenuti costi esterni** per affrontare il caso, in quanto interventi di emergenza erano già previsti e inclusi nei contratti con i fornitori esistenti.
- Assicuratore e cliente hanno analizzato i dati di fatturazione per **verificare l’esistenza di un reale danno da interruzione dei canali di vendita**, non recuperabile nei giorni successivi al ripristino dell’infrastruttura tecnologica.
- Raggiunto un punto di incontro circa i criteri di analisi, l’Assicuratore ha emesso quietanza per il danno da interruzione di attività pari ad **€ 75.000 al netto della franchigia**.

Caso n.3: Errata gestione dei dati biometrici / Responsabilità verso Terzi

Azienda viene accusata di **errato trattamento di dati biometrici**, resi accessibili a terzi senza aver fatto sottoscrivere ai proprietari di tali dati **appositi moduli privacy** che specificassero tale aspetto. Viene instaurata una **Class action negli Stati Uniti**.

La polizza interviene rimborsando i **costi di difesa dell'azienda** e accettando di sostenere la **proposta di transazione definita con le controparti** per definire la Class action.

L'Assicuratore ha riconosciuto più di **€ 7.000.000** di danno.

Jacopo Gamba
Director Broking | FINEX Italy
Team Leader Cyber, Crime and Professional Indemnity

Direct: +39 02 47787361
Mobile: +39 340 3836804
jacopo.gamba@wtwco.com