CHUBB®

Gestire la velocità del rischio:

Intelligenza artificiale, contenziosi e resilienza

Cyber Claims Report 2026

Sezione 1

Introduzione: Un quadro eterogeneo

La natura del rischio Cyber continua a evolversi, mentre si intensifica l'ampiezza delle vulnerabilità e dell'esposizione al rischio. Grazie alla riuscita integrazione di sistemi di rilevamento basati sull'Intelligenza Artificiale (IA) e a una maggiore resilienza, diversi mercati globali hanno visto stabilizzarsi la frequenza degli incidenti Cyber nel 2025, secondo report recenti. Gli Stati Uniti, nel frattempo, hanno registrato un massimo storico in termini di gravità, con il costo medio di una violazione dei dati nel 2025 **superiore a $10.2 milioni** – oltre il doppio della media globale di $4.4 milioni.*

In definitiva, il successo di una singola azienda o di un mercato geografico nel proteggersi dagli incidenti Cyber dipende dalla comprensione dei seguenti fattori: un panorama di minacce in continua evoluzione, i quadri legali e normativi che regolano l'acquisizione e l'archiviazione dei dati e l'interconnessione tra i partner commerciali quale causa di aumento dell'esposizione lungo tutta la catena di fornitura di un'azienda, a monte e a valle.

Questa edizione del report Chubb Cyber Claims analizza i dati storici dei sinistri di Chubb fino a dicembre 2025, per offrire indicazioni sull'andamento della frequenza e della gravità dei sinistri e sui fattori che alimentano tali tendenze. Con l'obiettivo di aiutare le aziende a orientarsi in un contesto di rischio Cyber complesso e a rafforzare la loro resilienza finanziaria e operativa.

*Fonte: *IBM Cost of Data Breach Report 2025*

Sezione 2

Tendenze globali dei sinistri

In tutti i mercati, l'aumento dei sinistri Cyber è stato trainato dai cambiamenti tecnologici e dal nuovo scenario normativo, oltre che dall'interconnessione delle supply chain. Tre tendenze che emergono con chiarezza.

01

L'IA accelera la velocità del rischio.

La stessa tecnologia di IA che ha permesso di individuare gli incidenti Cyber in modo più rapido e approfondito ha cambiato radicalmente la velocità con cui si sviluppano gli attacchi. Integrando l'IA agentica e autonoma nei malware, i criminali oggi riescono a compromettere più sistemi nel giro di pochi minuti – riducendo quasi a zero lo spazio per un intervento manuale. L'uso di IA avanzata da parte dei criminali, come i Large Language Models (LLM), sta crescendo quasi alla stessa velocità dell'adozione dell'IA da parte dei consumatori.

02

Il riflesso del "litigation-first".

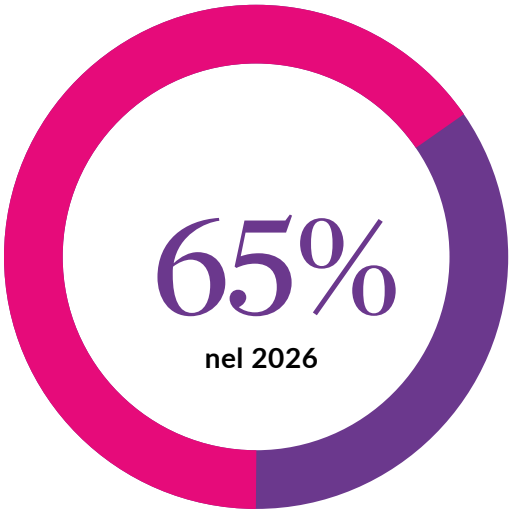
Un incidente Cyber non è più soltanto un guasto tecnico da risolvere: spesso diventa il detonatore di un'azione legale poco dopo l'evento. Negli ultimi 30 anni, le leggi su privacy e protezione dei dati sono state introdotte a un ritmo straordinario, aumentando la complessità della conformità e la frequenza dei contenziosi in materia di privacy. Il divario tra una violazione e il primo deposito di una class action si è ridotto: spesso la causa parte nel giro di pochi giorni, con accuse diverse a prescindere dalle dimensioni dell'organizzazione o dai controlli ritenuti mancanti.

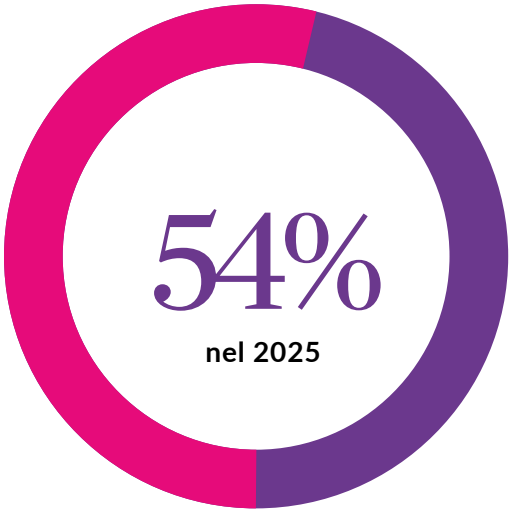
03

Interdipendenza sistemica.

Fino a pochi anni fa, i responsabili del rischio si concentravano soprattutto sull'evitare che i propri guasti informatici avessero ripercussioni su clienti e fornitori. Oggi è diffusa la consapevolezza del forte impatto che la supply chain dell'organizzazione può avere sulla frequenza e sulla gravità degli incidenti informatici.

Secondo il World Economic Forum, oggi il 65% delle grandi aziende considera le vulnerabilità di terze parti e della supply chain la principale sfida in ambito Cyber, in aumento rispetto al 54% nel 2025.





Incidente informatico presso un produttore automobilistico globale

Come illustrato più avanti nel dettaglio, episodi come l'incidente informatico che ha colpito un grande costruttore automobilistico globale nell'agosto 2025 hanno messo in evidenza i pesanti effetti economici e operativi che un attacco Cyber può avere a qualsiasi livello della catena di fornitura. L'evento ha provocato un'ondata d'urto in tutta l'economia britannica, generando in un attimo ripercussioni diffuse. Oltre alle ingenti perdite finanziarie subite dal produttore per i fermi produttivi, oggi esso deve anche affrontare numerose azioni legali collettive legate all'incidente.

Sezione 3

Frequenza e gravità degli incidenti informatici

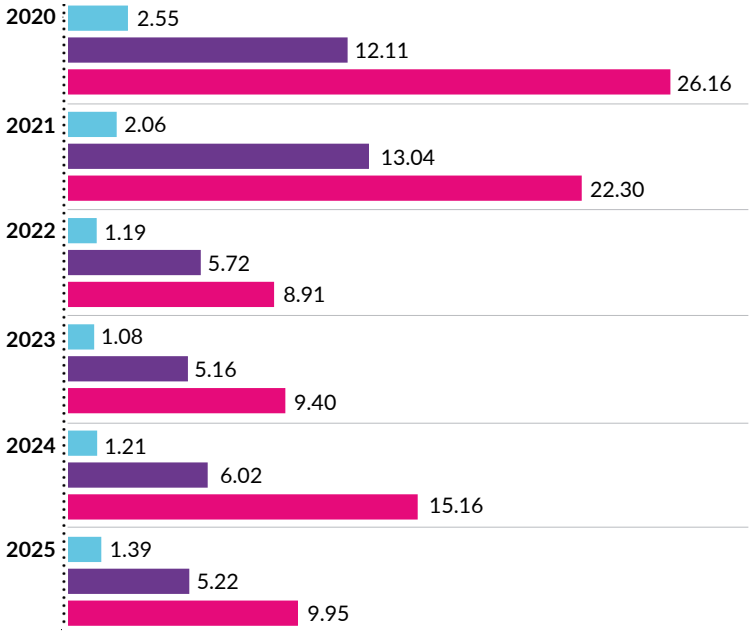
La frequenza, ossia il numero di sinistri per polizza, e la severità, cioè il costo medio per sinistro, sono gli elementi fondamentali che vanno a determinare i costi dei sinistri assicurativi e i principali fattori che guidano le variazioni dei premi assicurativi. Poiché l'assicurazione, per sua natura, è un'attività in cui il premio applicato segue con ritardo il costo reale dei sinistri, i trend storici più recenti di frequenza e severità rappresentano un indicatore anticipatore delle tariffe per l'anno successivo.

Le tabelle a lato mostrano un quadro eterogeneo dei trend di frequenza e severità nel panorama Cyber statunitense negli ultimi sei anni.

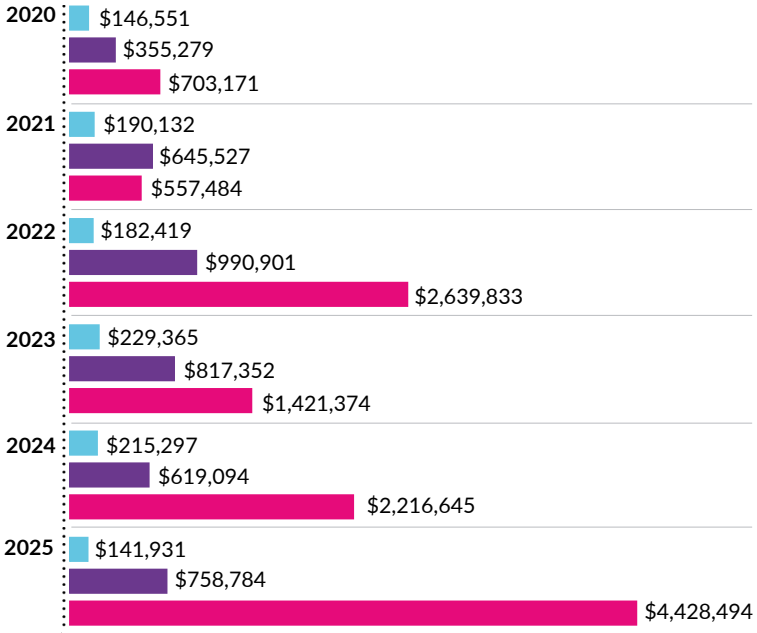
I miglioramenti nei profili di sicurezza dei clienti e nelle capacità di resilienza si riflettono nella marcata riduzione della frequenza dei sinistri tra aziende di ogni dimensione tra il 2020 e il 2022. Allo stesso tempo, i dati evidenziano un aumento complessivo della frequenza tra le Piccole e Medie Imprese (PMI) e nei gruppi di rischio delle grandi aziende dal 2022, mentre il segmento middle-market è rimasto più stabile nello stesso periodo.

L'utilizzo dei massimali è diminuito dal 2021, anche se la severità è aumentata. Se nel segmento PMI la severità è rimasta sostanzialmente stabile, è cresciuta in modo significativo nel segmento middle-market e ancora più nettamente nel segmento dei grandi clienti. A questo aumento contribuiscono diversi fattori, tra cui l'incremento dei costi per interruzione di attività e l'aumento delle spese legali legate sia alle violazioni dei dati sia ai contenziosi sulla privacy.

Frequenza dei sinistri Cyber ogni 100 polizze (USA)

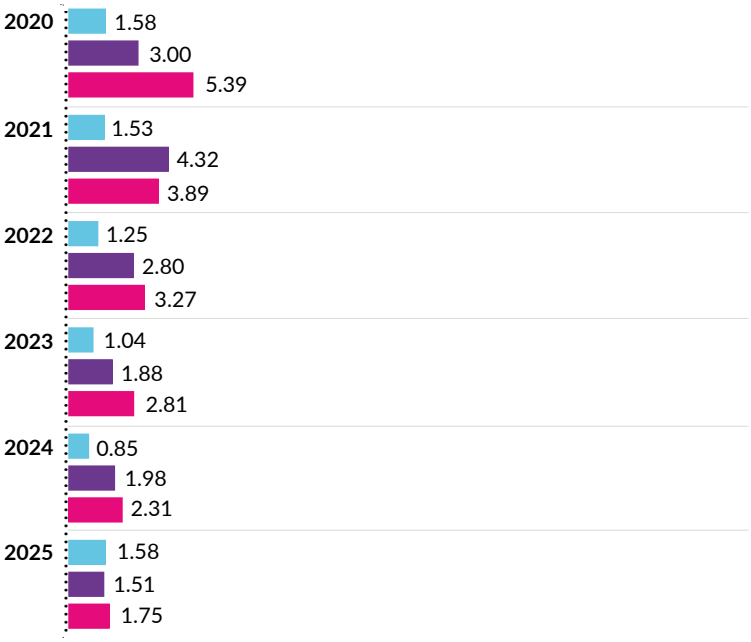


Gravità media dei sinistri Cyber (USA)

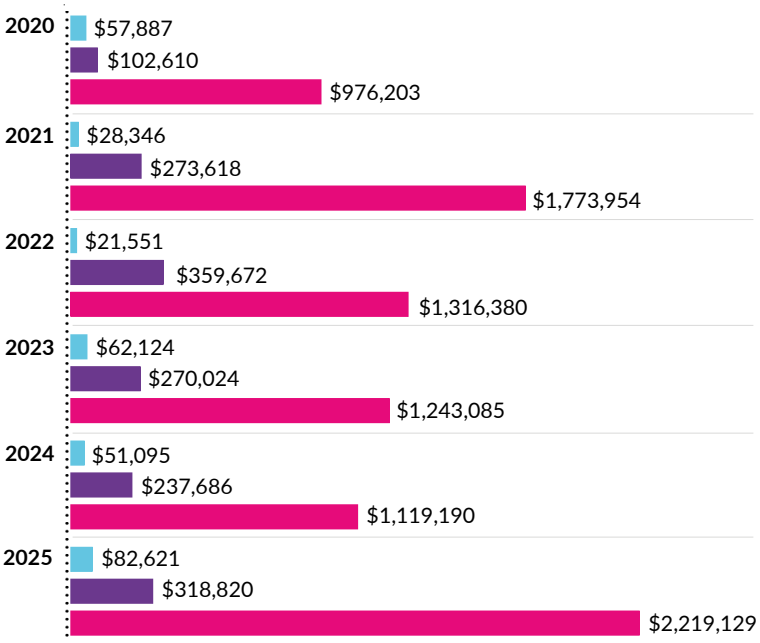


PMI: fatturato $0-$99M
Middle-market: fatturato $100M-$999M
Grandi clienti: fatturato $1B+

Frequenza dei sinistri Cyber ogni 100 polizze (Europa + Regno Unito)



Gravità media dei sinistri Cyber (Europa + Regno Unito)



PMI: fatturato $0-$99M
Middle-market: fatturato $100M-$999M
Grandi clienti: fatturato $1B+

Le tendenze in Europa e nel Regno Unito mostrano analogie e differenze rispetto agli USA.

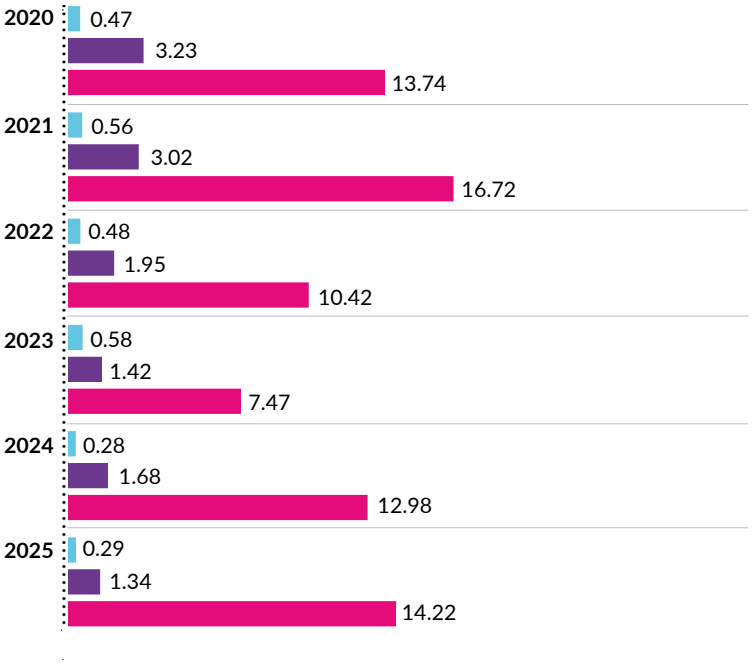
I livelli di frequenza sono simili nella coorte delle PMI, ma molto più bassi nei segmenti middle market e grandi clienti. Questo indica che la probabilità di subire un attacco, così come il profilo di sicurezza generale e i controlli in essere, sono comparabili tra le PMI negli USA, in Europa e nel Regno Unito. Dall'altro lato, si osserva una netta riduzione dell'esposizione nei segmenti delle aziende medie e grandi in Europa e nel Regno Unito rispetto agli USA, dovuta in larga parte all'assenza di sinistri legati a contenziosi con terze parti.

La severità è più bassa in tutte le coorti europee e del Regno Unito, anche in questo caso soprattutto per l'assenza di spese rilevanti di contenziosi con terze parti, sia per violazioni dei dati sia per sinistri privacy senza data breach. Pur essendo evidente l'aumento della severità in tutte le coorti, questa rimane più stabile rispetto agli USA.

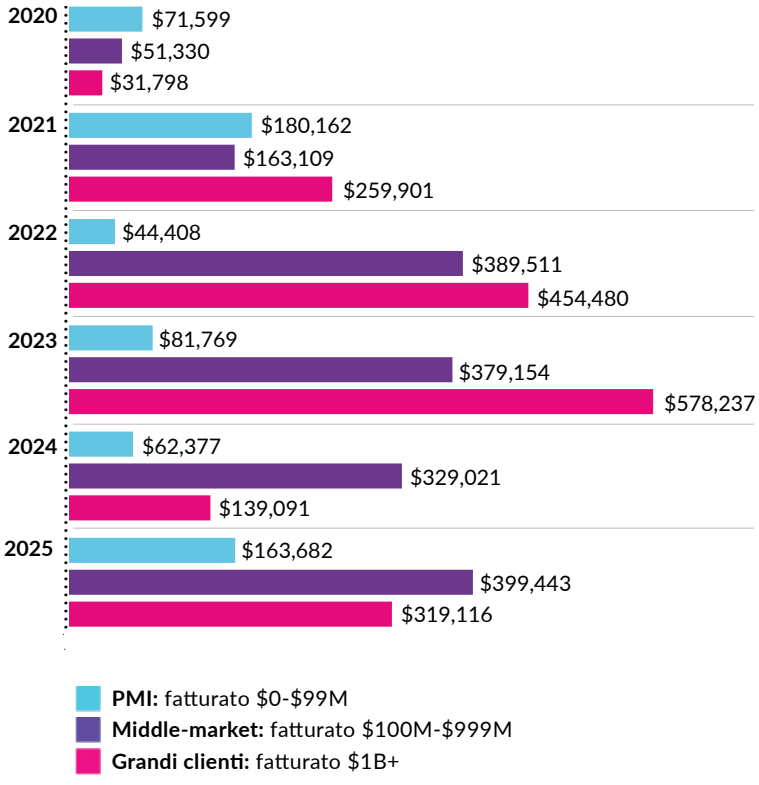
In Australia e Nuova Zelanda i livelli assoluti di frequenza e di gravità, così come l'andamento complessivo, differiscono rispetto ad altre aree del mondo, ma seguono la stessa traiettoria generale.

La frequenza è diminuita in modo marcato, mentre la gravità in generale è aumentata dopo il 2021. La frequenza per le PMI rappresenta solo una frazione dei livelli osservati in altre aree del mondo, ma la gravità è sostanzialmente in linea. La frequenza nel segmento middle-market è in linea con Europa e Regno Unito – ed è molto più bassa rispetto agli USA – riflettendo un contesto normativo relativamente favorevole per le azioni legali legate a violazioni di dati Cyber e per le iniziative sulla privacy non legate a data breach. Da segnalare inoltre che i segmenti middle-market e grandi clienti hanno registrato livelli di gravità più contenuti, con aumenti più moderati nel tempo.

Frequenza dei sinistri Cyber ogni 100 polizze (Australia e Nuova Zelanda)



Gravità media dei sinistri Cyber (Australia e Nuova Zelanda)



Sezione 4

La corsa agli armamenti dell'Intelligenza Artificiale: Attacco e Difesa

La crescente diffusione e l'evoluzione dell'IA a livello globale hanno portato a un uso malevolo della tecnologia sempre più sofisticato, ma anche a strumenti efficaci per il rilevamento e la mitigazione.

I prodotti assicurativi Cyber di Chubb coprono incidenti informatici di ogni tipo, compresi quelli legati all'IA. Le alternative di mercato alla copertura esplicita – come clausole specifiche sull'IA, sottolimiti o garanzie più ristrette – andrebbero valutate con attenzione da assicurati e broker.

Un esempio: a novembre, Anthropic – la società che ha sviluppato lo strumento di IA Claude – ha riferito di essere stata vittima di "una campagna di spionaggio altamente sofisticata" condotta da criminali che hanno sfruttato le capacità agentiche dell'IA in misura senza precedenti.

L'IA non è stata usata soltanto come consulente, ma per eseguire gli stessi attacchi informatici. L'operazione, che ha preso di mira grandi aziende tecnologiche, istituti finanziari e agenzie governative, tra le altre organizzazioni, è stata, secondo Anthropic, "il primo caso documentato di un cyberattacco su larga scala eseguito senza un intervento umano significativo".

Tra gli altri sviluppi nell'uso ostile dell'IA agentica e del malware autonomo rientrano:

- Nuove varianti capaci di riscriversi durante l'esecuzione per eludere il rilevamento basato su firme.
- Sciami autonomi di ricognizione – "cavallette digitali" – che mappano intere reti aziendali e avviano attacchi mirati dopo avere individuato all'istante le vulnerabilità.
- IA che affina e ottimizza deepfake iper-realistici per imitare con precisione le voci dei CFO o di altri dirigenti e indurre i dipendenti a effettuare trasferimenti di fondi non autorizzati.

Inoltre, continuano episodi legati all'IA meno complessi, come quando un dipendente carica per errore Informazioni di Identificazione Personale (PII) su un LLM (un modello di IA) accessibile pubblicamente, provocando un incidente informatico.

Per difendersi, aziende e organizzazioni possono adottare strumenti di mitigazione del rischio collaudati e incentrati sull'IA, per rispondere a queste minacce e ridurre la propria esposizione.

Ecco alcuni strumenti di difesa:

Difese AI-first: adottare operazioni di sicurezza guidate dall'IA (AISO) per individuare le minacce in tempo reale.

Governance dell'IA: mantenere un inventario rigoroso di tutti i sistemi di IA e verificare le pratiche di gestione dei dati dei fornitori terzi.

Formazione potenziata: formare i dipendenti sui rischi di sicurezza legati all'IA, come phishing avanzato e deepfake.

Sezione 5

L’impatto delle frodi di ingegneria sociale

Le richieste di risarcimento per frodi di social engineering possono essere molto pesanti, soprattutto per le piccole e medie imprese. Il rischio di perdite economiche, interruzioni operative e danni reputazionali evidenzia quanto siano indispensabili strategie efficaci di risposta e di ripristino.

Caso di sinistro Cyber per frode tramite social engineering

L'evento: dopo aver ricevuto un'email che sembrava provenire da un rappresentante di un fornitore storico di macchinari, un nuovo dipendente modifica le coordinate bancarie per il pagamento al fornitore, indirizzandolo su un nuovo conto, senza prima verificare l'autenticità del messaggio chiamando il fornitore in ufficio.

L'impatto: solo in seguito l'azienda si rende conto che il dipendente è caduto vittima di una frode di social engineering, quando il vero referente del fornitore sollecita il pagamento e si scopre che l'email era fraudolenta e che il versamento era stato effettuato a un impostore.

$100.000

La soluzione: Perdita superiore a $100.000. Nessun recupero né dalla banca né dal fornitore.

L'esito: la polizza Cyber, con un'estensione per i crimini informatici, rimborsa l'assicurato per le perdite non recuperabili.

Sezione 6

La frontiera della privacy e il riflesso del "litigation-first"

Con il crescente numero di incidenti informatici che si trasformano in vere e proprie vicende legali, le aziende si trovano ad affrontare nuove sfide giuridiche legate a inedite teorie di responsabilità, soprattutto in materia di intercettazioni e tecnologie di tracciamento digitale.

I principali fattori che incidono sulla responsabilità legale includono:

Il riflesso "prima il contenzioso": negli Stati Uniti, gli avvocati dei querelanti stanno sfruttando leggi sulle intercettazioni vecchie di decenni (come il **California Invasion of Privacy Act**) e norme sulla privacy dei video (come il federale **Video Protection Privacy Act**) per colpire tecnologie web standard, incluso il tracciamento tramite pixel.

Normative su dati e privacy: il quadro normativo sulla privacy, in continua evoluzione nel Regno Unito e in Europa, il **Regolamento generale sulla protezione dei dati (GDPR)** e il **Data (Use and Access) Act 2025 (DUAA)** che si basa sul **UK Data Protection Act**, hanno creato obblighi complessi per le aziende nella gestione dei dati personali, incluso l'uso di tecnologie web standard, come i pixel di tracciamento.

Arbitrati di massa: negli Stati Uniti, le aziende sono costrette a pagare ingenti costi amministrativi anticipati per ogni singola istanza. In una causa con 10.000 querelanti, per esempio, queste spese non rimborsabili possono superare i $10 milioni prima ancora che il merito della controversia venga esaminato.

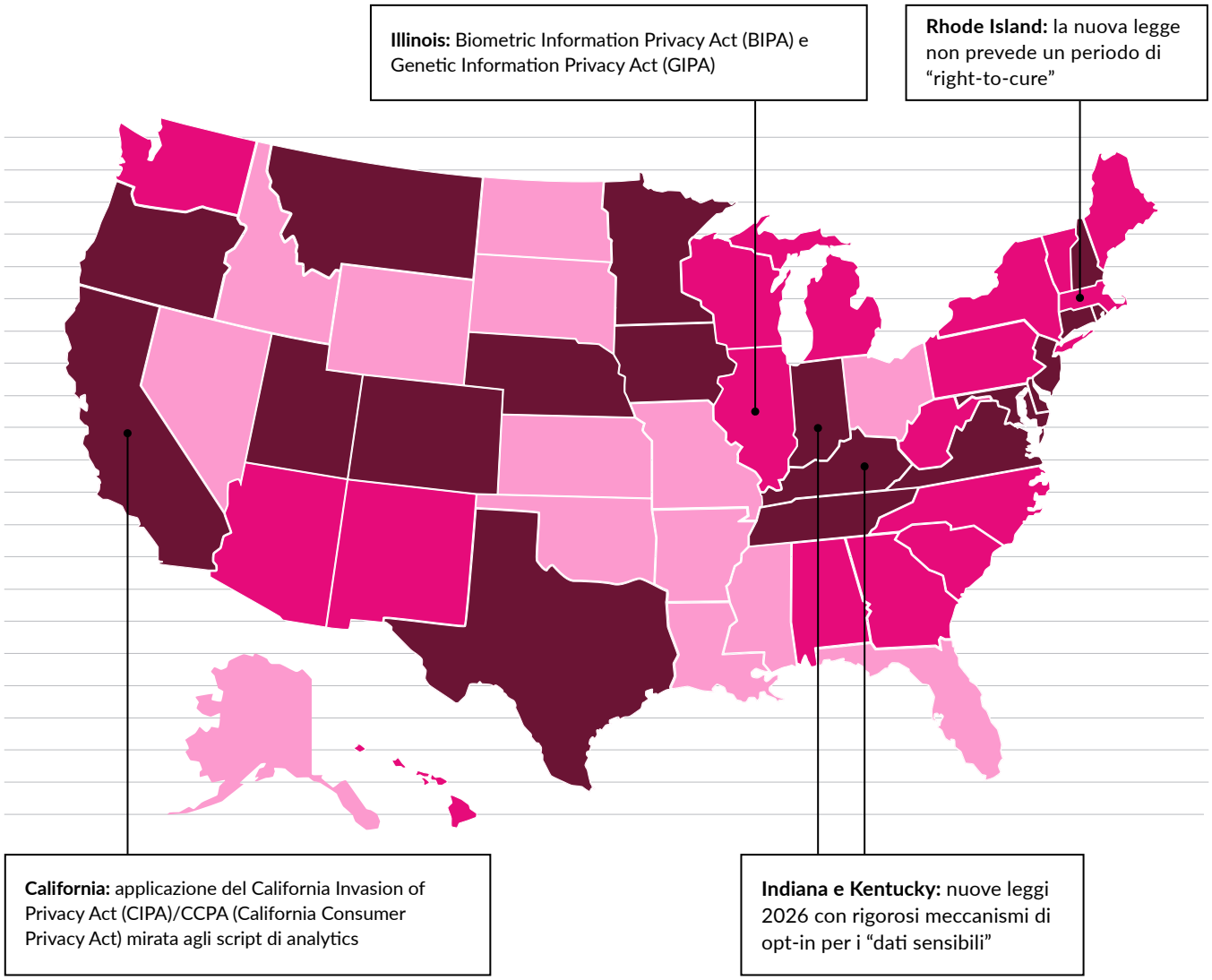
Soppressione dei dati: i criminali stanno passando a cancellare o divulgare intenzionalmente i dati, invece di limitarsi a cifrarli – creando una "perdita di controllo" permanente – che può aumentare la posta in gioco nei contenziosi.

Un numero crescente di norme sulla privacy negli Stati Uniti e nell'UE sta imponendo obblighi complessi e stratificati alle aziende che conservano e/o trasferiscono dati personali. Tra questi rientrano il diritto di opporsi alla profilazione o alle decisioni automatizzate, obblighi di trasparenza per trattamenti basati su IA, e valutazioni del rischio obbligatorie per i casi d'uso ad alto rischio.

Stati Uniti

Monitoraggio della normativa sulla privacy

Non esiste una normativa federale, ma un mosaico di regolamentazioni a livello statale.



Fonte: *US Federal Privacy Legislation Tracker*

Per le aziende nel Regno Unito e in Europa, è importante tenere conto di questo mosaico di regolamentazioni statali quando si opera con o negli Stati Uniti. Per saperne di più, visita **Chubb Cyber Insurance**.

Sezione 7

Protezione dei dati sensibili

Gli incidenti legati alla privacy stanno diventando una fonte sempre più rilevante di sinistri Cyber, sia per frequenza sia per gravità. Con normative in continua evoluzione e l'aumento delle cause su larga scala, gestire il rischio privacy è oggi più complesso e costoso. Ogni azienda può trovarsi ad affrontare sfide diverse nel proteggere i dati, in uno scenario di minacce in costante cambiamento.

Gestire i rischi legati alla privacy dei consumatori e garantire la conformità normativa è fondamentale. Per supportare i nostri assicurati, Chubb ha avviato partnership con piattaforme di gestione del rischio privacy che consentono agli assicurati di proteggere le proprie organizzazioni valutando e gestendo in modo proattivo i rischi per la privacy, tutelando i dati sensibili e mantenendo la conformità.

Caso di sinistro privacy nel segmento Middle-Market

L'evento: l'assicurato gestisce un sito web in abbonamento e un'app mobile che utilizzano tecnologie di tracciamento, inclusi cookie e pixel. Il pixel rileva alcuni dati, tra cui l'ID utente del visitatore del sito, e li trasmette a terze parti.

L'impatto: numerosi studi legali hanno inoltrato migliaia di richieste pre-arbitrato sostenendo che l'uso del pixel violasse il California Invasion of Privacy Act, che vieta l'intercettazione delle comunicazioni senza consenso.

$40M+

Il problema: La privacy policy dell'assicurato prevedeva che tutte le controversie dovessero essere risolte tramite arbitrato. Tuttavia, il regolamento dell'organismo arbitrale avrebbe imposto all'assicurato il pagamento di diversi milioni di dollari in spese iniziali di deposito, prima ancora di valutare il merito delle richieste. Di conseguenza, se i reclami fossero stati arbitrati, avrebbero potuto comportare un potenziale risarcimento previsto per legge, oltre alle spese arbitrali, per un totale superiore a $40 millioni.

La soluzione: Chubb ha incaricato legali con esperienza in contenziosi in materia di privacy e nei rapporti con gli studi legali, favorendo così l'avvio di una mediazione della controversia.

$6.5M

L'esito: i molteplici reclami sono stati risolti complessivamente per un importo nell'ordine di $6.5 millioni.

Sezione 8

L’impatto del ransomware sulle piccole e medie imprese

Gli attacchi ransomware continuano a rappresentare rischi rilevanti per le piccole e medie imprese (PMI), spesso con conseguenti violazioni dei dati complesse e onerose. Anche quando i primi tentativi di cifratura vengono bloccati, l’esfiltrazione di informazioni sensibili può far scattare ampi obblighi di notifica e interventi di ripristino.

Chubb vanta una solida esperienza nella gestione dei sinistri ransomware e offre servizi legali, di informatica forense, di pubbliche relazioni e altri servizi specialistici per supportare i suoi assicurati nel gestire con efficacia gli incidenti ransomware: riparando o sostituendo i sistemi danneggiati, riducendo al minimo i tempi di inattività e tornando rapidamente operativi.

Caso di sinistro ransomware per PMI

L'evento: i tentativi di un gruppo di criminali di cifrare il computer dell'assicurato sono stati in gran parte bloccati dallo strumento di endpoint detection and response dell'assicurato. Tuttavia, il criminale informatico è riuscito a esfiltrare informazioni sanitarie e i numeri di previdenza sociale di oltre 4 milioni di persone.

L'impatto: l'assicurato doveva identificare rapidamente e con precisione quali dati e quali informazioni sanitarie personali fossero stati compromessi, per rispettare gli obblighi di notifica previsti da leggi e regolamenti applicabili.

Il problema: comprendere l'entità della violazione dei dati, garantire una notifica tempestiva alle persone interessate e assicurare che le vulnerabilità non corrette potenzialmente sfruttate venissero risolte il più rapidamente possibile.

$4M

La soluzione: sono stati incaricati immediatamente un consulente legale, un team forense e un team di data mining per supportare l'assicurato nella gestione dell'evento. Dopo un'analisi approfondita dei dati coinvolti, sono stati informati 4 milioni di individui e numerose autorità di vigilanza dell'accaduto. È stato inoltre coinvolto il team Risk Advisor di Chubb per aiutare il cliente ad affrontare le vulnerabilità non ancora corrette.

$4.7M

Il risultato: il costo totale rimborsato all'assicurato è stato di $4.7 milioni, inclusi $2.4 milioni per le spese di notifica e $1.2 milioni per i costi di monitoraggio del credito a favore delle persone coinvolte. L'assicurato è stato inoltre informato delle vulnerabilità non ancora corrette e supportato nelle attività di remediation.

Sezione 9

Ransomware senza confini

Gli attacchi ransomware continuano a rappresentare un rischio serio per le organizzazioni in tutto il mondo. Anche le istituzioni con misure di cybersicurezza avanzate possono subire gravi interruzioni quando i criminali informatici sottraggono dati sensibili e li rendono pubblici. Le conseguenze spesso si estendono oltre i confini nazionali, attivando controlli regolatori, obblighi legali e sfide operative.

Come dimostra questo episodio in Europa, il ransomware non conosce confini geografici.

Caso di sinistro ransomware a livello globale

L'evento: un attacco ransomware condotto da un gruppo di threat actor, allora sconosciuto, ha colpito un'istituzione accademica internazionale e il suo ramo editoriale. Oltre 575.000 documenti sensibili sono stati esfiltrati e successivamente pubblicati sul sito di leak del gruppo.

L'impatto: le operazioni sono state interrotte a livello globale. Dati sensibili, tra cui i compensi degli autori, ricerche governative e tracce di esami futuri, sono stati esposti in oltre 40 Paesi. Il ripristino si è rivelato particolarmente complesso nelle aree con dipendenze IT articolate.

Il problema: l'istituzione accademica ha dovuto valutare tutti i 575.000 documenti sottratti per stimare il rischio normativo. È stato necessario un supporto legale in 40 giurisdizioni, aumentando sensibilmente complessità e pressione per rispettare i requisiti di conformità a livello globale.

La soluzione: Chubb ha messo in campo esperti legali e forensi e un data mining avanzato ha individuato i contenuti a più alto rischio, consentendo una revisione rapida, in gran parte automatizzata. Il coordinamento dei pareri legali tra continenti ha garantito notifiche regolatorie puntuali e accurate.

$14.2M

Il risultato: la perdita complessiva è stata di $14.2 milioni, includendo i costi di risposta all'incidente informatico e le perdite da interruzione dell'attività. Grazie a un intervento rapido e a un supporto legale coordinato, l'istituzione accademica ha evitato multe, indagini regolatorie o sanzioni. Nonostante l'ampiezza della violazione, gli impatti reputazionali e normativi sono stati contenuti con successo.

Sezione 10

Eventi a impatto diffuso: i costi a catena dell'interdipendenza

Nessuna azienda opera in totale isolamento: si appoggia a partner, fornitori e clienti. Due cyberattacchi di rilievo del 2025 mostrano quanto i danni di un attacco ransomware possano coinvolgere più imprese lungo l'intera supply chain di un'azienda. Se Chubb aveva già lanciato l'allarme su questo tema nel 2022, oggi la gravità di questi eventi risalta con sempre maggiore chiarezza in tutto il panorama della cybersecurity.

Regno Unito – agosto 2025

Produttore automobilistico globale

L'attacco di fine agosto 2025 a un produttore automobilistico globale è il più devastante incidente informatico nella storia britannica. I dettagli dell'evento sono un monito, con lezioni fondamentali per tutte le aziende.

L'incidente

Attribuito ai "Scattered Lapsus Hunters", l'attacco ha imposto la disattivazione delle reti IT globali per contenere la violazione.

L'impatto operativo

La produzione si è fermata per cinque settimane in vari stabilimenti nel Regno Unito, in Slovacchia, Brasile e Cina. Tra i sistemi andati in stallo c'erano i controlli delle linee di produzione, le apparecchiature di progettazione CAD/PLM e le piattaforme di ordinazione dei concessionari.

Le conseguenze su sicurezza e fronte legale

Gli hacker hanno sottratto dati sulle buste paga e archivi clienti a 7,4 milioni di persone, dando il via a un contenzioso su larga scala.

Le ripercussioni finanziarie sistemiche

£1.9B

Economia

L'economia del Regno Unito ha registrato una perdita stimata di £1.9 miliardi ($2.5 miliardi), contribuendo a un rallentamento del PIL nel Q3 2025.

£1.2B

Impatto sulla supply chain

Oltre 5.000 organizzazioni nel Regno Unito sono state colpite; il governo è intervenuto con £1.2 miliardi in prestiti d'emergenza per stabilizzare la filiera.

£485M

Danni dell'azienda

Il produttore automobilistico globale ha registrato danni ante imposte per £485 milioni, ribaltando un utile di £398 milioni rispetto all'anno precedente.

Stati Uniti – febbraio 2025

Violazione dei dati di Oracle Health

All'inizio del 2025, Oracle Health (in precedenza Cerner) ha subito una grave violazione dei dati che gli analisti hanno giudicato tra le più imponenti nella storia del settore sanitario statunitense.

L'incidente

I criminali informatici hanno usato credenziali rubate per accedere ai server legacy di migrazione dati di Cerner, non ancora trasferiti su Oracle Cloud.

La vulnerabilità principale

La violazione ha colpito un ambiente legacy – in parte inutilizzato dal 2017 – dimostrando che i dati "dimenticati" sono un bersaglio privilegiato.

L'impatto

L'attacco ha sottratto i dati di circa 80 ospedali, esponendo i numeri di previdenza sociale dei pazienti e le loro cartelle cliniche, incluse diagnosi e immagini dei trattamenti.

Il ricatto

Un attore malevolo che operava con l'alias Andrew ha preteso milioni in criptovaluta per impedire la divulgazione dei file sottratti.

Questi e altri eventi del 2025 – inclusi molti dovuti a errori o incidenti più che a intenzioni dolose (ad es., l'interruzione in ottobre di Amazon Web Services) – evidenziano quanto sia necessario individuare e adottare le più rigorose misure disponibili per mitigare il rischio informatico.

Sebbene questi scenari possano sembrare lontani dalle piccole imprese, l'esperienza di Chubb dimostra che la realtà è ben diversa.

Caso di sinistro per una PMI tramite fornitore terzo

L'evento: il retailer assicurato si era affidato a un fornitore tecnologico terzo per il software indispensabile alle attività quotidiane. Quando il fornitore è stato colpito da un attacco ransomware, tutti i suoi sistemi sono andati offline.

L'impatto: non potendo utilizzare il software, l'assicurato non è riuscito a vendere alcuni prodotti, ordinare le scorte o programmare gli appuntamenti con i clienti.

La soluzione: Chubb ha incaricato un commercialista forense di supportare l'assicurato nel calcolo della conseguente perdita per interruzione di attività dipendente da terzi. La preparazione dell'assicurato, grazie al piano di risposta agli incidenti e all'integrazione con la gestione sinistri di Chubb, ha contribuito a gestire un evento in gran parte fuori dal suo controllo.

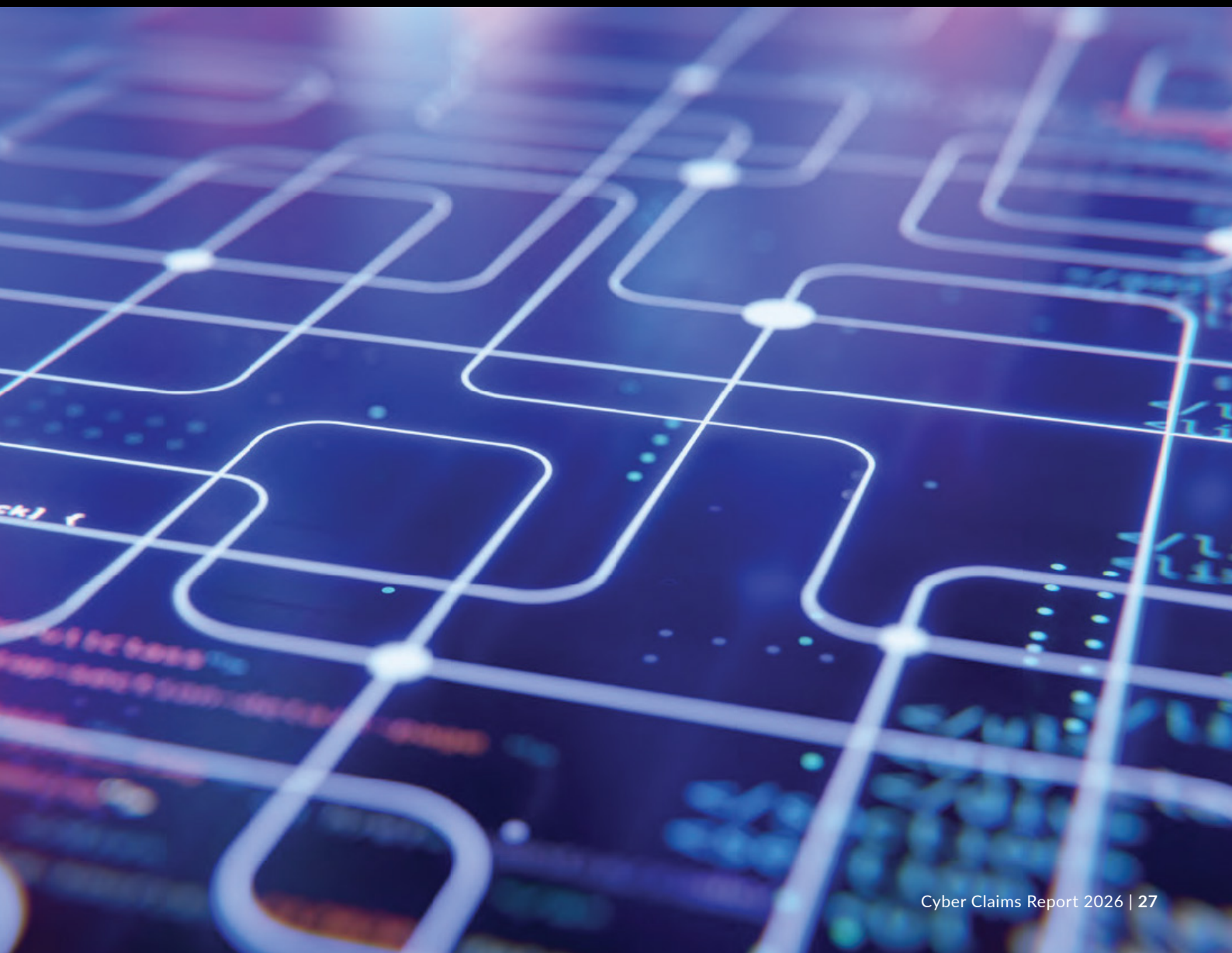
$1.2M

Esito: la perdita complessiva è stata di $1.2 milioni.

Sezione 11

Chubb: aiutare le aziende con informazioni utili per ridurre il rischio Cyber

Oltre agli strumenti di riduzione del rischio, la conoscenza è una delle difese migliori contro minacce informatiche in continua evoluzione. Chubb mette a disposizione degli assicurati una serie di approfondimenti per supportare la prevenzione e la mitigazione degli incidenti Cyber.



Chubb Cyber Index

Il Cyber Index di Chubb, lanciato nel 2015, offre accesso in tempo reale ai dati proprietari globali sui sinistri di Chubb e a informazioni utili sulle minacce informatiche attuali, sui trend e sui costi.

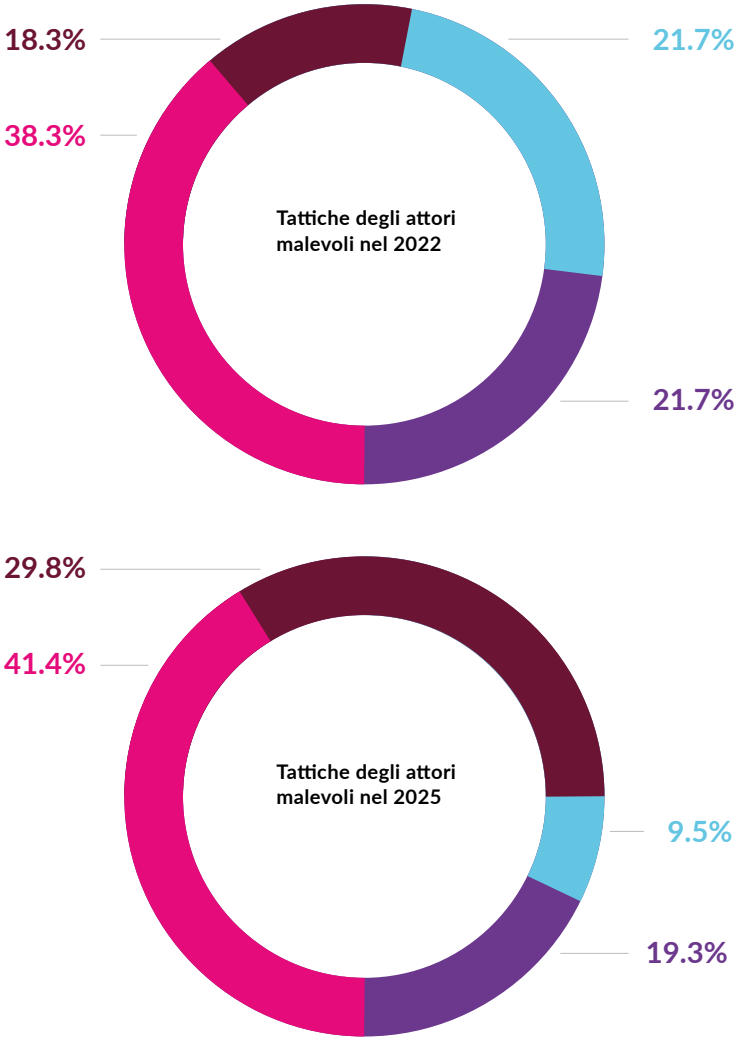
La piattaforma di ricerca consente agli utenti di impostare parametri e visualizzare gli andamenti storici in base a:

Attività degli incidenti: analisi delle tendenze delle minacce Cyber che colpiscono le aziende, per dimensione, settore e area geografica.

Costi dei sinistri: analisi dei costi dei sinistri Cyber di Chubb in base alla dimensione dell'azienda e al settore.

Calcolatore del rischio Cyber: uno strumento che offre una visione più ampia delle esposizioni Cyber e dei potenziali costi delle perdite Cyber.

Insight sugli acquisti dei peer: consentono alle aziende di confrontare la propria protezione Cyber con quella di aziende simili.



Rispetto al 2022, la quota di sinistri derivanti dallo sfruttamento di vulnerabilità gravi è scesa da quasi il 22% al 9% – in linea con il lancio, da parte di Chubb, del programma di Outreach per la gestione delle vulnerabilità, con cui il nostro team di Cyber Threat Intelligence dà priorità alle vulnerabilità sfruttabili più critiche e invia avvisi mirati solo agli assicurati potenzialmente interessati da tali vulnerabilità. Il servizio è offerto gratuitamente a tutti gli assicurati Cyber di Chubb.

Chubb Threat Intelligence

Oltre al nostro Cyber Claims Report, Chubb pubblica un Threat Intelligence Report trimestrale per offrire ai professionisti della sicurezza informatica indicazioni sintetiche e operative sugli ultimi sviluppi delle minacce Cyber e sull'esperienza di Chubb nella gestione dei sinistri.

Un report recente ha evidenziato che, nel 2025, la tecnica di accesso iniziale più frequente alla base di un incidente ransomware è stata il phishing. Al secondo posto l'abuso di servizi remoti esposti (ad es. uso improprio della VPN, porte aperte), mentre al terzo si sono collocati gli exploit di vulnerabilità critiche.

Attraverso il nostro programma di Outreach per la gestione delle vulnerabilità, Chubb esegue costantemente la scansione del proprio portafoglio e informa broker e assicurati di criticità gravi e sfruttabili che richiedono l'applicazione di patch, sia al rinnovo sia durante il periodo di validità della polizza. Questo servizio è offerto gratuitamente a tutti i titolari di polizze Cyber di Chubb.

Oltre al nostro programma di Outreach per la gestione delle vulnerabilità, Chubb offre servizi mirati al phishing, pensati per aiutare gli assicurati a ridurre l'esposizione agli attacchi di phishing, tra cui:

Formazione

Corsi e giochi di sensibilizzazione alla sicurezza e prevenzione del phishing per i dipendenti, basati sulle minacce più recenti.

Test

Simulazioni di email di phishing, incluse simulazioni con tecnologia deepfake, per valutare il processo decisionale dei dipendenti.

Tecnologia

Uno strumento di sicurezza email basato sull'Intelligenza Artificiale per aiutare a individuare l'intento di phishing, il linguaggio e le anomalie comportamentali che a una persona potrebbero sfuggire.

CHUBB®

Affidati a Chubb per una protezione Cyber completa e una resilienza solida.

Chubb European Group SE, Sede legale: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Francia - Capitale sociale €896.176.662 i.v.- Rappresentanza generale per l'Italia: Via Fabio Filzi n. 29 - 20124 Milano - Tel. 02 27095.1 - Fax 02 27095.333 – P.I. e C.F. 04124720964 – R.E.A. n. 1728396 – Abilitata ad operare in Italia in regime di stabilimento con numero di iscrizione all'albo IVASS I.00156. L'attività in Italia è regolamentata dall'IVASS, con regimi normativi che potrebbero discostarsi da quelli francesi. Autorizzata con numero di registrazione 450 327 374 RCS Nanterre dall'Autorité de contrôle prudentiel et de résolution (ACPR) 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 RCS e soggetta alle norme del Codice delle Assicurazioni francese. info.italy@chubb.com - www.chubb.com/it