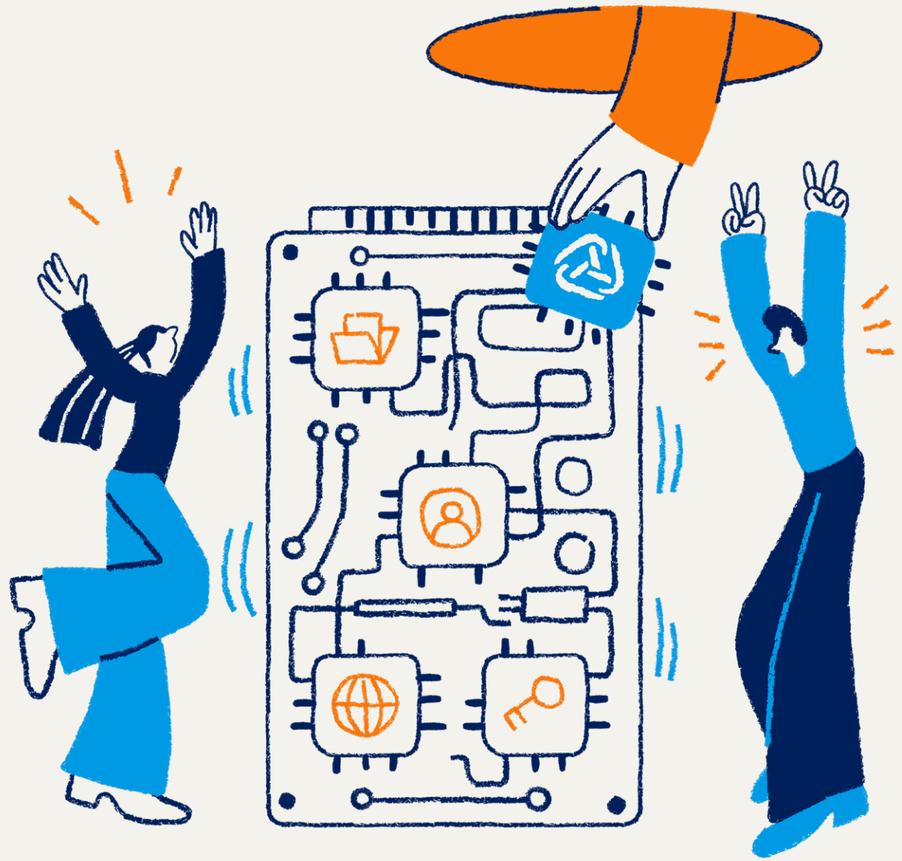
QBE Insurance

La nuova anatomia del rischio cyber



At the heart of it

Come dipendenze, concentrazioni e lacune nei sistemi di controllo possono trasformare un incidente cyber in una crisi operativa

Tre punti chiave

La resilienza informatica dipende dalla capacità di gestire le dipendenze critiche per il business con lo stesso rigore applicato ai sistemi di controllo della sicurezza informatica.

1

Le vulnerabilità più comuni possono trasformare un incidente cyber in un'interruzione prolungata dell'operatività.

2

La capacità di ripristino è essa stessa un elemento cruciale della resilienza.

3

Executive summary

La resilienza informatica dipende oggi sempre più dalla capacità di gestire le dipendenze critiche per il business. Le organizzazioni fanno ampio affidamento su ecosistemi digitali interconnessi, infrastrutture cloud e fornitori di software essenziali per le loro attività, ma spesso al di fuori del loro controllo diretto. Di conseguenza, la capacità di un'organizzazione di resistere a un'interruzione e ripristinare le proprie attività è sempre più legata alla tenuta delle complesse reti di fornitori e partner di servizi da cui dipende.

Tre cambiamenti che stanno ridefinendo il rischio cyber

1. **Velocità:** gli attaccanti passano dall'accesso iniziale allo sfruttamento della vulnerabilità nell'arco di pochi minuti, anziché di giorni. Le organizzazioni hanno quindi sempre meno tempo per individuare un attacco e reagire.
2. **Concentrazione:** è aumentata la dipendenza dei settori critici da un numero relativamente ristretto di provider cloud, piattaforme software e fornitori di servizi. Un'interruzione che coinvolge uno dei principali operatori può quindi avere ripercussioni su più settori e Paesi contemporaneamente.
3. **Convergenza:** la crescente integrazione tra tecnologie informatiche (IT), tecnologie operative (OT) e dispositivi connessi amplia le possibili conseguenze degli incidenti cyber, con il rischio di compromettere anche operazioni fisiche e servizi essenziali.

Le tensioni geopolitiche stanno intensificando l'attività cyber

I conflitti in Europa e Medio Oriente sono stati accompagnati da un aumento delle operazioni cyber di natura distruttiva, rivolte contro infrastrutture critiche, servizi pubblici e grandi organizzazioni.

Le forme di guerra ibrida rendono inoltre sempre più sfumato il confine tra conflitto geopolitico e attività criminale. Sanità, trasporti, logistica, tecnologia e altri settori di rilevanza strategica sono diventati bersagli sempre più frequenti. Alla fine del 2025, ad esempio, la Russia ha condotto un attacco su larga scala contro il settore energetico polacco in pieno inverno, con l'obiettivo di provocare gravi interruzioni.

Non tutte le interruzioni hanno origine dolosa

Le interruzioni che hanno interessato Amazon Web Services nell'ottobre 2025 e Cloudflare nel novembre dello stesso anno hanno avuto ripercussioni simultanee su piattaforme bancarie, retail, di trasporto e di servizi pubblici in diversi mercati. In entrambi i casi, un problema a un'infrastruttura condivisa si è propagato ai numerosi servizi che dipendevano da essa. La resilienza sistemica è quindi fondamentale, indipendentemente dal fatto che un'interruzione sia provocata da un attacco criminale o da un malfunzionamento dell'infrastruttura.

I governi stanno rafforzando la risposta alla minaccia

Governi e autorità di regolamentazione stanno intervenendo per rafforzare la sicurezza delle supply chain, la resilienza operativa, la segnalazione degli incidenti e la pianificazione del ripristino. Unione Europea, Regno Unito e Canada, ad esempio, hanno recentemente introdotto normative volte a rafforzare i requisiti relativi al controllo dei fornitori, alla verifica dei piani di ripristino e alla segnalazione degli incidenti.

Parallelamente, le preoccupazioni legate alla sovranità digitale, alla dipendenza tecnologica e alla competizione strategica stanno portando all'introduzione di nuove restrizioni in materia di tecnologia, dati e attività digitali transfrontaliere.



La sfida delle PMI

Le PMI rappresentano una sfida importante per governi, assicuratori e operatori della sicurezza informatica. Le grandi organizzazioni sono sottoposte a crescenti pressioni normative e commerciali affinché dimostrino la propria resilienza cyber. Le PMI, invece, dispongono spesso di minori risorse interne, pur facendo affidamento su molte delle stesse tecnologie e supply chain interconnesse.

Sensibilizzazione e supporto concreto diventano quindi fondamentali. Rafforzare la resilienza cyber non richiede necessariamente investimenti significativi in nuove tecnologie. Misure relativamente semplici, come l'autenticazione a più fattori e sistemi di backup efficaci, possono migliorare sensibilmente la capacità di un'azienda di affrontare un incidente.

Per le organizzazioni più grandi, si tratta anche di una questione di supply chain: aiutare i fornitori più piccoli a rafforzare la propria resilienza contribuisce, in ultima analisi, a tutelare la continuità operativa delle aziende che dipendono da loro.

Cinque raccomandazioni per rafforzare la resilienza

1. **Sicurezza proattiva:** adottare l'autenticazione a più fattori (MFA) e correggere tempestivamente le vulnerabilità.
2. **Governance e responsabilità:** definire a livello di senior management la propensione al rischio e attribuire chiaramente la responsabilità della sua gestione.
3. **Gestione delle dipendenze:** identificare i servizi critici e i fornitori da cui dipendono, definendo modalità alternative per garantirne il ripristino.
4. **Test ed esercitazioni:** verificare regolarmente le procedure di ripristino e coinvolgere il management in esercitazioni su possibili scenari di crisi.
5. **Preparazione e risposta:** assicurarsi in anticipo l'accesso alle competenze necessarie in ambito forense, legale e comunicazione di crisi, preparando il management a prendere decisioni in situazioni di emergenza.

La cyber insurance come servizio

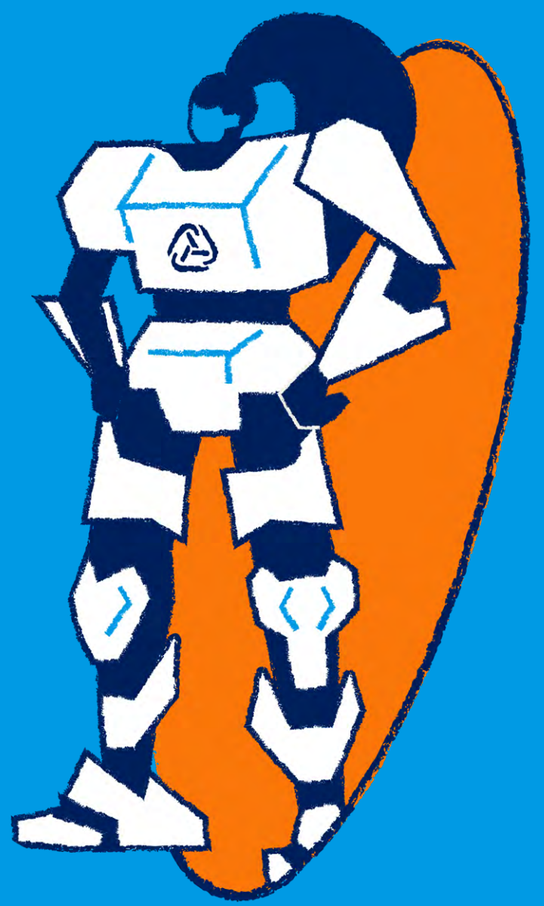
Le aziende non dovrebbero considerare l'assicurazione cyber esclusivamente come uno strumento finanziario che interviene dopo un sinistro. La polizza può rappresentare anche una porta di accesso a competenze specialistiche prima, durante e dopo un incidente. Broker e assicuratori possono aiutare le organizzazioni a comprendere meglio la propria esposizione, individuare gli ambiti in cui è utile rafforzare la resilienza e sfruttare al meglio i servizi specialistici a loro disposizione.

Introduzione: quando la dipendenza supera la capacità di controllo

Man mano che il numero di potenziali punti di accesso aumenta, la resilienza informatica è sempre più strettamente legata alla resilienza complessiva dell'organizzazione. In un contesto in cui le aziende dipendono sempre più da sistemi digitali interconnessi, una strategia di sicurezza informatica efficace deve andare oltre la prevenzione degli attacchi, per comprendere come un'interruzione possa propagarsi all'interno dell'organizzazione e quanto rapidamente sia possibile ripristinare le attività critiche.

La maggior parte delle organizzazioni è consapevole del fatto che gli attacchi informatici possono causare gravi interruzioni dell'attività aziendale. Ciò che è meno chiaro è perché le stesse tipologie di attacco abbiano oggi conseguenze più gravi sulle organizzazioni colpite rispetto a tre anni fa. Secondo una recente indagine di settore, un attacco ransomware comporta oggi in media, per un'organizzazione colpita, 24 giorni di interruzione operativa come conseguenza diretta dell'attacco[1], mentre un'altra stima indica che, per gli incidenti più gravi, il ripristino complessivo può richiedere dai tre ai sei mesi.[2][3]

La spiegazione non risiede solo nella crescente capacità degli aggressori, ma anche nei profondi cambiamenti dell'ambiente in cui operano le organizzazioni, che indeboliscono le difese e ampliano la superficie di attacco. La vulnerabilità alle minacce cyber della continuità operativa è sempre più legata al grado di dipendenza delle organizzazioni da sistemi digitali sui quali non hanno il pieno controllo, ma dei quali non possono fare a meno. Un ulteriore elemento determinante è la capacità di individuare queste dipendenze e di pianificare misure adeguate per affrontare eventuali interruzioni.



1 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
2 https://www.accenture.com/en/insights/security/redefining-cyber-resilience
3 Per "interruzione operativa" si intende un'interruzione di sistemi, reti o applicazioni causata da un incidente cyber. Per "ripristino complessivo" si intende il processo di ripristino dei sistemi interessati, riportandoli a uno stato sicuro e pienamente operativo dopo un incidente.

Sono tre i fattori che, insieme, hanno contribuito ad aggravare il rischio e ampliato il divario tra dipendenza dalle tecnologie e controllo su di esse:

Velocità

Negli ultimi anni i tempi di esecuzione degli attacchi si sono notevolmente ridotti, limitando il margine di tempo a disposizione delle organizzazioni per

> "Gli attori delle minacce possono ora passare [...] allo sfruttamento (della vulnerabilità) in appena 30 minuti."

individuarli e contenerli. Questa accelerazione è probabilmente dovuta, almeno in parte, alla crescente disponibilità di strumenti e piattaforme avanzate basate sull'intelligenza artificiale. Ad esempio, una recente indagine ha rilevato che una campagna basata sull'IA ha condotto in meno di dieci ore un attacco coordinato su larga scala che avrebbe richiesto a un operatore umano circa due settimane per essere organizzato.[4] Altri studi indicano inoltre che gli autori delle minacce sono ora in grado di passare dall'accesso iniziale allo sfruttamento della vulnerabilità in soli 30 minuti, rispetto ai circa 100 minuti del 2021.[5]

Concentrazione

In tutti i settori e in tutte le aree geografiche, i processi di digitalizzazione hanno favorito la concentrazione di sistemi e funzioni su infrastrutture condivise, con l'obiettivo di ottimizzare e semplificare le risorse digitali aziendali. Ad esempio, nel 2025 AWS, Microsoft Azure e Google Cloud hanno rappresentato quasi i due terzi della spesa delle aziende per i servizi di infrastruttura cloud.[6] Dato che la velocità della digitalizzazione e dell'interoperabilità hanno la priorità rispetto ai sistemi di controllo, i servizi critici si affidano sempre più a un numero ristretto di fornitori di servizi cloud, suite Software-as-a-Service (SaaS), piattaforme di gestione delle identità e fornitori di servizi gestiti (MSP), aumentando così il rischio di interruzioni che, partendo da un singolo nodo critico, possano propagarsi a cascata tra aziende e settori.

> "La digitalizzazione spinta ha favorito la concentrazione dei sistemi."

Convergenza

Gli ambienti IT, Operational Technology (OT) e dell'Internet delle cose (IoT) sono sempre più interconnessi, mentre la gestione delle identità tende a concentrarsi presso un unico fornitore. Di conseguenza, una singola violazione può ora coinvolgere più domini che prima erano separati.

Il risultato è che anche comuni carenze nella gestione dei controlli – come la mancata richiesta di autenticazione a più fattori (MFA), un server legacy senza patch o una rete non segmentata – possono propagare gli effetti di un attacco all'interno dell'organizzazione in modo più vasto e rapido. In particolare, il 90% delle violazioni analizzate in una recente ricerca è risultato riconducibile a carenze evitabili, come una visibilità limitata sui sistemi, controlli applicati in modo incoerente e un'eccessiva fiducia nei meccanismi di gestione delle identità.[7]

La resilienza mostra i suoi limiti quando il livello di dipendenza supera quello di controllo; concentrazione e convergenza amplificano inoltre la portata e la gravità delle conseguenti interruzioni. Per costruire una solida resilienza informatica, le organizzazioni devono tenere conto di entrambi questi aspetti.

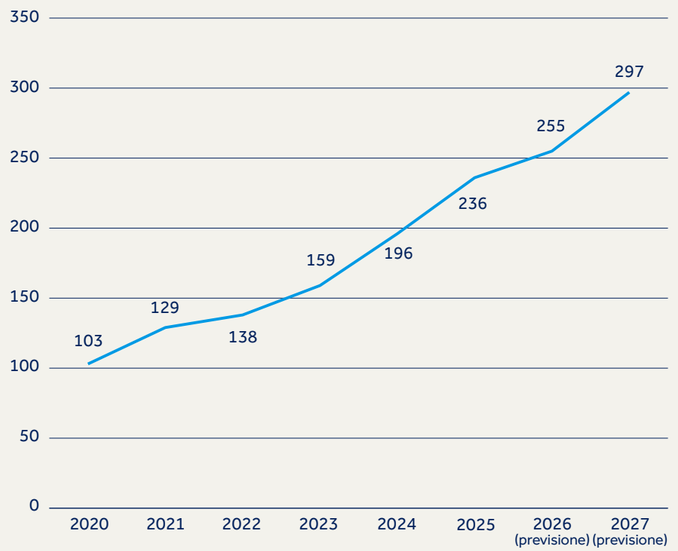
4 https://unit42.paloaltonetworks.com/ai-assisted-cyber-attack-inside-a-unit-42-investigation/
5 https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/
6 Synergy Research Group: nel terzo trimestre del 2025 AWS, Microsoft Azure e Google Cloud hanno rappresentato il 63% della spesa aziendale per i servizi di infrastruttura cloud. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher
7 https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

Sfide parallele: intenti dirompenti, impatti dirompenti

Nei 14 mercati QBE analizzati (si veda Ambito di applicazione e note), dal 2023 il numero di incidenti che provocano interruzioni operative è aumentato ogni anno e si prevede che aumenti ancora nel 2027.[9] Ciò che è cambiato non è solo il numero di episodi, ma anche il loro impatto: rispetto a tre anni fa, quando gli incidenti causavano in genere qualche giorno di interruzione, oggi è più probabile che l'interruzione si protragga più a lungo, perché sono molte di più le attività aziendali che dipendono dai sistemi colpiti.

Dietro questa tendenza ci sono tre fattori chiave: un ecosistema criminale ormai maturo, che ha reso sempre più professionali l'accesso ai sistemi, gli strumenti di attacco e le tecniche di negoziazione; la frammentazione geopolitica e l'aumento delle attività ibride, che rendono sempre più sfumato il confine tra azioni riconducibili a Stati e attività criminali; e l'industrializzazione dell'intelligenza artificiale, che probabilmente contribuisce ad accorciare i tempi di azione degli attaccanti e rende più semplice mettere in atto campagne di social engineering convincenti. Ad esempio, alcuni studi indicano che le e-mail di phishing personalizzate, generate dall'intelligenza artificiale e inviate attraverso processi automatizzati, raggiungono un tasso di clic del 54%. Un risultato in linea con quello ottenuto dalle e-mail di phishing personalizzate create dall'uomo, che richiedono però agli attaccanti più tempo e risorse, e significativamente superiore al 12% registrato dai tentativi generici elaborati manualmente.[10]

Figura 1: Numero di incidenti informatici dirompenti di rilevanza strategica (2020-2027)[11]



Fonte: Control Risks. Vedere la sezione "Ambito di applicazione e note" per le regioni, la metodologia di raccolta dei dati e i limiti

"Gli attacchi informatici non si limitano a compromettere le informazioni; possono bloccare l'operatività delle organizzazioni, con costi medi nell'ordine di milioni.[8] In quasi tutti i casi di cui ci occupiamo, il fattore decisivo non è quanto sia sofisticata l'intrusione, ma quanto l'attività aziendale dipende dal sistema colpito e quanto l'organizzazione fosse preparata e avesse pianificato la gestione di un'interruzione di quel sistema."

Responsabile della Cyber Threat Intelligence, Digital Risks, Control Risks

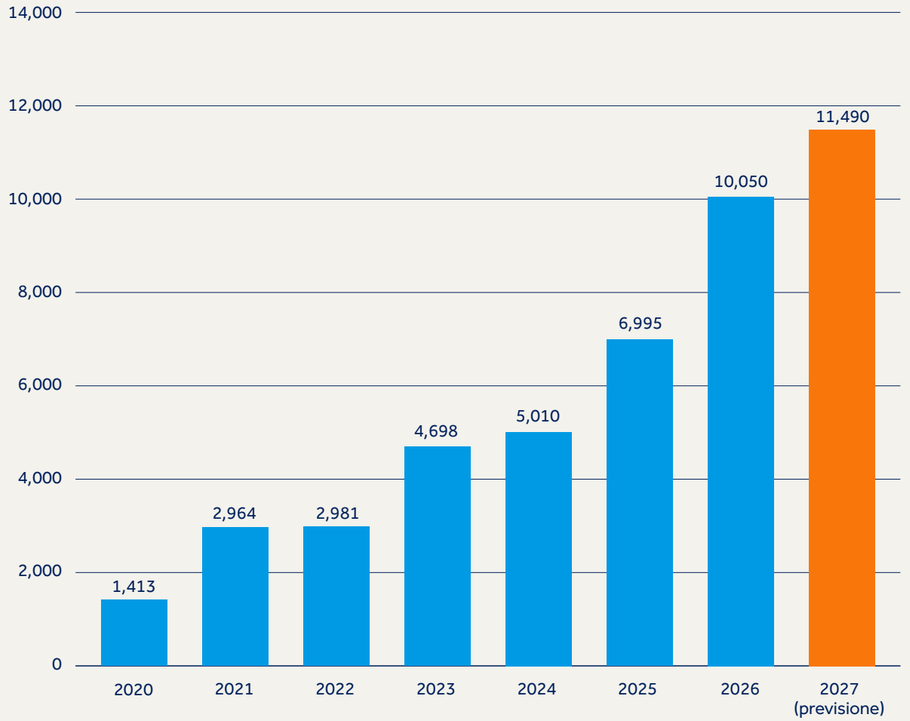
8 Ad esempio, il rapporto di IBM "Cost of Data Breach 2026" indica che una violazione costa in media alle vittime 4,99 milioni di dollari, https://www.ibm.com/reports/data-breach
9 Il numero complessivo nei 14 mercati
10 https://www.researchgate.net/publication/386374220_Evaluating_Large_Language_Models'_Capability_to_Launch_Fully_Automated_Spear_Phishing_Campaigns_Validated_on_Human_Subjects
11 Questi dati si basano su una raccolta selezionata di incidenti che soddisfano uno o più criteri, tra cui il tipo di organizzazione presa di mira, l'autore della minaccia, la natura dell'attacco e i suoi obiettivi, nonché l'impatto.

Le estorsioni criminali continuano a imperversare…

Il ransomware e le estorsioni basate sulla sottrazione e sulla minaccia di diffusione di dati rimangono tra le minacce informatiche più costose dal punto di vista finanziario e potenzialmente più destabilizzanti che le organizzazioni devono affrontare. Nel tentativo di massimizzare l'impatto delle proprie azioni, i criminali prendono sempre più spesso di mira fornitori terzi noti, la cui compromissione può avere ripercussioni su numerosi clienti e aumentare la pressione durante le trattative per il pagamento del riscatto. Le grandi aziende dei settori manifatturiero, della vendita al dettaglio, dei servizi professionali e dell'IT sono spesso bersaglio di operazioni cyber criminali volte a provocare interruzioni dell'attività, nelle quali gli attaccanti sfruttano l'elevata interconnessione delle catene di fornitura. Ad esempio, si stima che l'attacco ransomware con sottrazione ed estorsione di dati subito nel 2024 da Change Healthcare, uno dei principali operatori statunitensi nell'elaborazione dei pagamenti in ambito sanitario, abbia provocato oltre 2 miliardi di dollari tra costi diretti e danni indiretti.[12]

Secondo le ricerche di Control Risks, il numero di organizzazioni vittime indicate sui siti utilizzati dai gruppi ransomware per pubblicare i dati sottratti è aumentato del 611% tra il 2020 e il 2026 e si prevede un'ulteriore crescita del 14% nel 2027.

Figura 2: Numero di organizzazioni vittime citate sui siti che divulgano dati relativi ai ransomware a livello globale (2020-2027)



Fonte: dati di Control Risks relativi agli incidenti e alle informazioni di intelligence. Vedere la sezione "Ambito di applicazione e note" per le regioni, la metodologia di raccolta dei dati e i limiti

12 https://hyperproof.io/resource/understanding-the-change-healthcare-breach/

…e le tensioni geopolitiche rendono la sfida ancora più ardua

L'escalation delle tensioni geopolitiche in Europa e in Medio Oriente ha coinciso con un aumento delle operazioni ibride, comprese quelle informatiche, volte a causare disagi. Nel 2025 e nel 2026 sono stati osservati attacchi contro infrastrutture critiche e brand di primo piano condotti da attori statali come Russia e Iran. Nei 14 mercati QBE esaminati, è probabile che questi fattori geopolitici continuino a esercitare la propria influenza nel medio-lungo periodo.

A questo si potrebbero aggiungere picchi di attività nel breve termine legati a eventi come le elezioni di medio termine negli Stati Uniti a novembre 2026 e le elezioni francesi del 2027, in linea con le dinamiche di interferenza elettorale osservate da almeno un decennio. Di conseguenza, le aziende che operano in queste giurisdizioni continueranno a essere esposte a minacce n grado di mettere alla prova la loro resilienza digitale.

> "Alla fine del 2025, la Russia ha condotto un attacco distruttivo su larga scala contro il settore energetico polacco, nel pieno dell'inverno.."

Nonostante le loro intenzioni distruttive siano diventate sempre più evidenti, gli Stati continuano a cercare di eludere ogni attribuzione di responsabilità, facendo sempre maggiore affidamento su gruppi cybercriminali e di attivisti informatici per colpire Paesi avversari senza un proprio coinvolgimento diretto e facilmente dimostrabile. Anche se la maggior parte di questi gruppi non è sotto il controllo diretto degli Stati, questi ultimi possono incoraggiarli, incentivarli o incaricarli direttamente di svolgere operazioni in linea con i propri interessi. Ad esempio, i ripetuti avvertimenti e le misure punitive adottate da diversi paesi europei nel 2026 indicano un significativo aumento del ricorso, da parte della Russia, all'ecosistema cybercriminale presente sul proprio territorio come strumento indiretto per colpire organizzazioni pubbliche e private in settori critici quali sanità, trasporti e logistica e fornitori IT.[13] Sebbene questi gruppi siano mossi principalmente da motivazioni economiche, il loro impatto destabilizzante contribuisce al raggiungimento di obiettivi strategici nell'ambito di campagne di guerra ibrida più ampie.

Sebbene le singole aziende possano non rappresentare l'obiettivo principale di attacchi distruttivi motivati da ragioni geopolitiche, gli incidenti che colpiscono fornitori di infrastrutture essenziali, come quelli del settore energetico o i fornitori IT critici, rischiano di avere ripercussioni significative a cascata. Ad esempio, alla fine del 2025 la Russia ha condotto in pieno inverno un attacco su larga scala contro il settore energetico polacco, sottolineando la sua intenzione di usare le operazioni informatiche per colpire direttamente la vita dei civili. Incidenti di così grande impatto sono stati storicamente rari, ma è probabile che diventino sempre più frequenti, sia per la crescente volontà di provocare interruzioni sia per l'elevato livello di interconnessione dei sistemi presi di mira. Minacce simili continueranno a provenire anche da attori proxy, sia criminali informatici che attivisti informatici, le cui capacità si stanno espandendo grazie al sostegno di attori statali e all'emergere di forme all'avanguardia di intelligenza artificiale.

13 https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/; https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions; https://www.lovguiden.dk/en/det-offentlige/eu-udenrigstjenesten/2026-07-21-eu-advarer-fn-om-ruslands-cyberproxyer-og-ransomware-mod-sundhedssektoren; https://www.rbb24.de/politik/beitrag/2026/02/krankenhaeuser-berlin-hybride-bedrohungen-russland-cyberangriffe.html ; https://therecord.media/ransomware-gangs-advancing-moscow-geopolitical-interests-warns-romania

La frammentazione geopolitica influenza la pianificazione della resilienza

Le tensioni geopolitiche hanno determinato anche cambiamenti sul piano normativo, con una crescente attenzione dei decisori politici alla sovranità digitale, alle restrizioni tecnologiche e alle limitazioni commerciali. Questo riguarda anche il settore dell'intelligenza artificiale, nel quale Stati Uniti e Cina continuano a competere per la leadership tecnologica e di mercato a livello globale. Dato che i cambiamenti normativi continuano a influire sugli accordi in merito alla privacy dei dati, sui requisiti di localizzazione e sulla disponibilità delle tecnologie, le aziende devono tenere sempre più conto dei vincoli normativi e dell'evoluzione delle politiche nella pianificazione della propria resilienza.

Ciò riguarda, ad esempio, la possibilità di ricorrere a fornitori alternativi per garantire la continuità operativa, così come la gestione delle più ampie problematiche di compliance che potrebbero emergere in uno scenario di crisi.

Visto che le minacce sistemiche dirompenti sembrano destinate a persistere, la resilienza operativa dipenderà dalla combinazione di preparazione aziendale, gestione del rischio legato a terze parti e solidità dei quadri nazionali di riferimento.

Figura 3: Analisi delle minacce e dello stato di preparazione nei 14 mercati oggetto dello studio

Mercati	Fattori geopolitici alla base delle minacce dirompenti[14]	Considerazioni sul livello dipreparazione[15]
Paesi nordici, Germania, Paesi Bassi, Francia, Regno Unito	Attività dirompenti condotte da attori allineati agli Stati e da attivisti informatici, legate alle tensioni tra Russia e NATO e dirette anche contro infrastrutture critiche	Quadri normativi nazionali maturi, ma esposizione delle tecnologie operative (OT) e delle infrastrutture critiche concentrata in pochi operatori
Stati Uniti e Canada	Elevato numero di attacchi informatici ritorsivi riconducibili all'Iran, legati al coinvolgimento degli Stati Uniti in Medio Oriente	Mercato consolidato dei servizi di risposta e ripristino, ma con capacità condivisa
Australia, Nuova Zelanda, Singapore, Hong Kong	Aumento delle attività legate ad attori statali e delle pressioni per un maggiore allineamento tra Washington e Pechino	In diversi mercati, le aspettative normative crescono più rapidamente rispetto alla capacità di risposta interna
Spagna e Italia	Attività di attivisti informatici filorussi legate alle posizioni politiche europee, con l'Italia regolarmente bersaglio di attacchi informatici di portata limitata	Ampia rete di fornitori composta da piccole imprese con livelli di maturità in materia di sicurezza disomogenei

Fonte: Analisi di intelligence di Control Risks. Per la metodologia di raccolta dei dati e i limiti vedere la sezione "Ambito di applicazione e note"

14 Questa sintesi si basa sui dati, sulle informazioni e sulla valutazione di Control Risks riguardo ai principali fattori geopolitici all'origine delle minacce informatiche dirompenti in queste aree.
15 Questa sintesi si basa sulla valutazione di Control Risks e su informazioni di terze parti relative agli aspetti chiave da considerare in merito al grado di preparazione in queste località, quali, tra gli altri fattori, i quadri normativi nazionali in materia di resilienza e preparazione, il livello di maturità del mercato della sicurezza informatica e la concentrazione/disponibilità dei fornitori.

Guasti alle infrastrutture senza un attacco

Non tutte le interruzioni sono dolose. I disservizi che hanno interessato Amazon Web Services (AWS) nell'ottobre 2025[16] e Cloudflare nel novembre dello stesso anno[17] hanno compromesso contemporaneamente il funzionamento delle piattaforme dei settori bancario, del commercio al dettaglio, dei trasporti e dei servizi pubblici in diversi mercati. In entrambi i casi, ciò è avvenuto a causa di un guasto relativo a un'infrastruttura condivisa che si è propagato a tutti i sistemi che dipendevano da essa. Nessuno dei due episodi è stato provocato da un attacco, ed è proprio questo a renderli particolarmente significativi: dimostrano come il rischio di concentrazione possa concretizzarsi indipendentemente dalla presenza di un attore ostile e senza che nessuno scelga deliberatamente un bersaglio. Anche per un'organizzazione priva di un rapporto contrattuale diretto con questi provider, le conseguenze pratiche possono essere le stesse: i suoi fornitori possono essere coinvolti e i tempi di ripristino possono dipendere da soggetti esterni.



16 Analisi di Ookla/Downdetector sull'interruzione del servizio AWS US-EAST-1 del 20 ottobre 2025: oltre 17 milioni di segnalazioni da parte degli utenti in più di 60 paesi e da oltre 3.500 aziende, con un impatto significativo durato circa 15 ore. https://www.ookla.com/articles/aws-outage-q4-2025
17 Interruzione del servizio Cloudflare del 18 novembre 2025: un errore di configurazione interno ha compromesso i servizi proxy e CDN a livello globale per circa 3,5 ore, influenzando una parte consistente del traffico Internet mondiale. https://blog.cloudflare.com/18-november-2025-outage/

I rischi legati alla concentrazione e la carenza di fornitori determinano il livello di esposizione

Figura 4: Dipendenze tecnologiche

Dipendenza tecnologica	A che punto siamo	Perché è importante
Cloud	AWS, Azure e Google Cloud rappresentano quasi i due terzi della spesa delle aziende per le infrastrutture cloud.[18]	Il malfunzionamento di un singolo fornitore comporta conseguenze correlate, e non isolate, in tutti i settori e mercati.
Terze parti	Nel 2025, la percentuale di violazioni che hanno coinvolto una terza parte è raddoppiata rispetto all'anno precedente, passando dal 15% al 30%.[19]	Sono i fornitori, più che il perimetro aziendale, a rappresentare oggi il vettore di ingresso in più rapida crescita.
Identità	Consolidamento dell'accesso su singoli fornitori che coprono gli ambienti IT, OT e SaaS	Una compromissione ora coinvolge ambiti che prima erano separati.
IA	L'adozione si è concentrata su un numero limitato di modelli, spesso privi dei controlli di accesso di base; secondo quanto riportato, il 77% delle aziende afferma che l'adozione dell'IA sta procedendo a un ritmo più veloce rispetto ai controlli.[20]	Nuove dipendenze vengono integrate più rapidamente di quanto si riesca a governarle.

Fonte: Analisi di Control Risks e dati di terze parti

I rischi qui esaminati sfuggono al controllo di qualsiasi singola organizzazione, ma determinano quanto lontano possano propagarsi le conseguenze di un malfunzionamento e quanto tempo possa richiedere il ripristino.

La crescente concentrazione su provider condivisi di servizi cloud, SaaS, gestione delle identità e Managed Service Provider (MSP) implica che un guasto o una compromissione presso un singolo fornitore possa avere un impatto simultaneo su tutte le organizzazioni che ne dipendono, direttamente o attraverso i propri fornitori. Per causare gravi disagi, quindi, non è più necessario che un'organizzazione sia l'obiettivo nè, nel caso di un guasto infrastrutturale, che esista un bersaglio vero e proprio. Per molte organizzazioni questa è la parte meno ben definita del quadro dei rischi, perché si colloca a metà strada tra la sicurezza, gli appalti e la continuità operativa, e non c'è una funzione specifica che se ne occupi.

Questa situazione comporta delle sfide strutturali che non possono essere completamente mitigate tramite garanzie contrattuali o ridondanze tecniche. Affidarsi a un ristretto gruppo di provider di tecnologia e piattaforme crea interdipendenze che vanno oltre il tradizionale rischio legato ai fornitori. Gli ecosistemi cloud moderni possono fare ampio affidamento su un unico fornitore per garantire l'intera gamma di servizi essenziali, creando così una situazione in cui il guasto di un singolo punto può causare interruzioni che coinvolgono più servizi all'interno di un'organizzazione. Il rischio di concentrazione viene ulteriormente amplificato dall'adozione dell'intelligenza artificiale, poiché la concentrazione nel settore dell'IA rispecchia e accresce le dipendenze già esistenti dal cloud e dalla tecnologia, dato che molte delle stesse aziende operano su entrambi questi servizi. Allo stesso tempo, questi rischi di concentrazione non possono essere completamente mitigati senza dover scendere a compromessi, che si tratti di capacità, interoperabilità o sicurezza.

Spesso si pensa che i fornitori di tecnologie critiche siano troppo importanti per subire interruzioni, il che porta molte organizzazioni a trascurare la propria capacità di resilienza. Ma episodi come le interruzioni di servizio del 2025 subite da AWS e Cloudflare dimostrano che nessuna tecnologia è completamente immune. Di conseguenza, le aziende (e le loro funzioni critiche) si ritrovano esposte a rischi quando non hanno previsto misure di ridondanza e piani di resilienza per i casi in cui i sistemi critici gestiti da terzi non siano disponibili.

18 Synergy Research Group: nel terzo trimestre del 2025 AWS, Microsoft Azure e Google Cloud hanno rappresentato il 63% della spesa aziendale per i servizi di infrastruttura cloud. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher
19 https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
20 https://newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-growing-ai-control-gap-as-enterprise-deployment-scales

Caso di studio: quando un’interruzione operativa si traduce in una perdita economica

L’attacco ransomware del 2025 che ha colpito un rivenditore con sede nel Regno Unito ha avuto un impatto stimato di 300 milioni di sterline sull’utile operativo e ha portato alla sospensione degli ordini online per 46 giorni, con il ripristino completo che si è protratto fino al 2026.[21] Si stima che la violazione subita nel 2023 dal produttore statunitense di beni di consumo Clorox abbia causato all’azienda danni per circa 380 milioni di dollari, di cui circa 50 milioni in costi di riparazione e il resto legato all’impossibilità di spedire i prodotti ai clienti.[22] In entrambi i casi, il vettore iniziale dell’attacco è stato legato alla supply chain, ma la compromissione ha determinato significative interruzioni operative, evidenziando il potenziale impatto delle più ampie dipendenze all’interno della catena di fornitura.

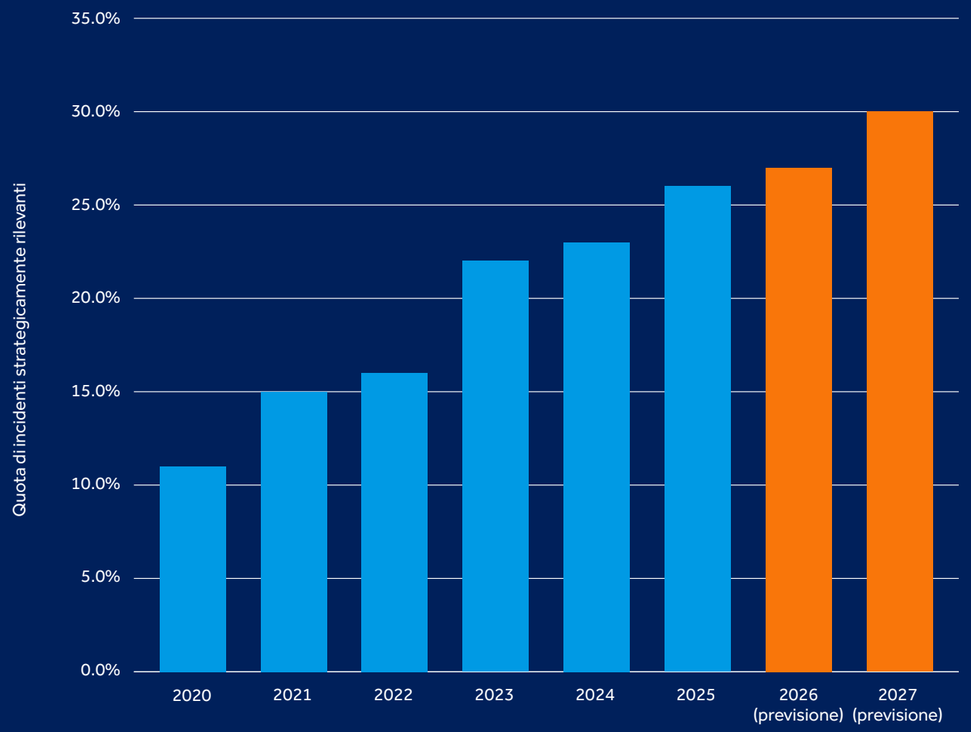
Negli ultimi due anni, Control Risks è intervenuta anche in alcuni casi in cui all’indomani di un attacco le aziende colpite sono state liquidate o vendute per somme irrisorie. Questo scenario trova riscontro anche in statistiche esterne, secondo cui il 60% delle piccole imprese prese di mira da attacchi informatici è costretto a cessare l’attività entro 6 mesi dall’incidente.[23] Il fattore determinante non è stato il livello di sofisticazione dell’intrusione, bensì il periodo durante il quale l’azienda non è stata in grado di operare: nel 2026, i tempi di fermo sono costati alle organizzazioni in media 15.000 dollari al minuto.[24]



21 Informazioni e rendiconti contestuali di Marks and Spencer Group plc, 2025-2026: un impatto stimato di 300 milioni di sterline sull’utile operativo dell’esercizio 2025/2026; ordini online sospesi dal 22 aprile al 10 giugno 2025. https://www.bbc.com/news/articles/c0el31nqnpvo
22 The Clorox Company contro Cognizant Technology Solutions, Corte Superiore della Contea di Alameda, luglio 2025: sono stati richiesti 380 milioni di dollari, di cui circa 49 milioni di dollari per i costi di ripristino e le perdite dovute all’interruzione dell’attività causate dall’attacco dell’agosto 2023. https://www.reuters.com/legal/government/clorox-accuses-it-provider-lawsuit-giving-hackers-employee-passwords-2025-07-22/
23 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
24 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026

La crisi dei fornitori: il problema va ben oltre il contratto

Figura 5: Aziende IT prese di mira in percentuale sul totale degli incidenti strategicamente rilevanti (2020-2027 previsioni)



Fonte: Analisi di Control Risks e dati di mercato di terze parti. Vedere la sezione "Ambito di applicazione e note" per le regioni, la metodologia di raccolta dei dati e i limiti

La concentrazione delle piattaforme è evidente. Quello che c'è sotto, invece, molto meno. L'esposizione va oltre i fornitori diretti, estendendosi ai loro subappaltatori e ai componenti software condivisi che poche organizzazioni riescono a mappare e, ancor meno, a monitorare. Queste dipendenze incidono tanto sul rischio di compromissione quanto sulle capacità di ripristino:

- **Singoli punti di vulnerabilità:** più servizi critici potrebbero dipendere da un'unica area cloud, da un'unica piattaforma SaaS o da un unico Managed Service Provider (MSP), spesso senza un'alternativa collaudata o un diritto contrattuale che garantisca priorità nelle attività di ripristino.
- **Maggiore dipendenza dalle supply chain:** i fornitori dei propri fornitori vengono raramente mappati, rendendo difficile per un'organizzazione rispondere a una domanda apparentemente semplice: chi altro deve essere operativo affinché possiamo continuare a esserlo anche noi?
- **Dipendenza nelle attività di ripristino:** i tempi di ripristino dipendono spesso da fattori esterni all'organizzazione, tra cui l'applicazione delle patch da parte dei fornitori, i tempi di ripristino previsti dal provider stesso o la piattaforma di backup di terze parti.
- **Caratteristiche dei backup:** eseguire regolarmente dei test di backup può ridurre i tempi di inattività in media di 15 giorni.[25] Tuttavia, alcune ricerche di settore indicano che il 94% delle vittime di ransomware utilizza sistemi di backup in parallelo con gli ambienti di produzione presi di mira dagli hacker, compromettendo potenzialmente le possibilità di ripristino proprio quando ne hanno più bisogno.[26]

25 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
26 https://fenix24.com/2026-state-of-recoverability-report/

La convergenza settoriale trasforma il malfunzionamento di un singolo fornitore in un evento che coinvolge l'intero settore

Settori diversi stanno convergendo verso le stesse piattaforme specialistiche, che si tratti di una suite SaaS dominante, di un fornitore OT comune o di un MSP condiviso, spesso a causa dei requisiti di certificazione, delle normative o delle aspettative dei clienti che restringono il campo dei fornitori idonei. Di conseguenza, il malfunzionamento di un singolo provider può interrompere contemporaneamente l'operatività di aziende concorrenti e, quando il disservizio coinvolge un intero settore, può venire meno anche la possibilità di affidarsi ad altri operatori dello stesso mercato per ottenere capacità o supporto alternativi.

> "Le autorità di regolamentazione hanno iniziato a considerare la questione come un problema sistemico."

Le autorità di regolamentazione hanno iniziato a considerare la questione come un problema sistemico piuttosto che legato alla sola gestione dei fornitori. La direttiva europea Network and Information Security 2 (NIS2) e il Digital Operational Resilience Act (DORA),[27] il previsto aggiornamento della normativa britannica in materia di cyber security e resilienza dei sistemi informativi e il Critical Cyber Systems Protection Act canadese introducono requisiti sempre più stringenti lungo l'intera catena di fornitura in materia di supervisione dei fornitori, verifica della continuità operativa e segnalazione degli incidenti. Le organizzazioni interessate da queste normative, così come il numero ben più ampio di quelle che le riforniscono, dovranno quindi prepararsi a dimostrare concretamente come gestiscono il rischio di concentrazione e la dipendenza da soggetti terzi nelle attività di ripristino, che diventeranno sempre più questioni di conformità normativa e non soltanto di valutazione interna.



27 Nel luglio 2026, Francia, Spagna e Paesi Bassi (tre dei 14 mercati QBE) non avevano ancora comunicato il recepimento completo della normativa, e la Commissione europea li ha deferiti (insieme all'Irlanda) alla Corte di giustizia. https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules La Cyberbeveiligingswet dei Paesi Bassi è poi entrata in vigore il 15 agosto 2026, attuando la direttiva NIS2. https://www.nldigitalgovernment.nl/dossiers/nis2-directive-cyberbeveiligingswet-cbw/

Quando gli incidenti si trasformano in crisi

Le carenze di sicurezza alla base degli incidenti che provocano interruzioni ricorrono con notevole continuità nel database di intelligence di Control Risks, che raccoglie informazioni provenienti da fonti aperte e dai casi in cui la società è intervenuta direttamente. Molte di queste vulnerabilità vengono aggravate dall'ampliamento delle superfici di attacco e dal potenziamento delle capacità degli autori delle minacce, comprese quelle rese possibili dall'intelligenza artificiale.

Cinque punti deboli ricorrenti trasformano gli incidenti in crisi



Identità, accessi e persone: l'assenza dell'autenticazione a più fattori (MFA), la possibilità di aggirarla, il riutilizzo delle credenziali e la presenza di account con privilegi eccessivi contribuiscono ad ampliare la superficie di attacco. Il social engineering basato sull'intelligenza artificiale sta inoltre rendendo più facile creare e diffondere tentativi di frode sempre più credibili, compresi quelli rivolti al personale dirigenziale, tecnico e di reparti chiave dell'azienda come risorse umane, ufficio legale e finanza.



Sistemi non aggiornati e obsoleti: la maggior parte delle vulnerabilità sfruttate nel 2025 erano problemi già noti e per i quali erano già disponibili delle soluzioni.[28] Nel 2026, l'utilizzo dell'intelligenza artificiale per individuare nuove vulnerabilità ha determinato un significativo aumento delle segnalazioni,[29] rendendo più complesso per le organizzazioni stabilire le priorità negli interventi di aggiornamento e applicazione delle patch.



Segmentazione inadeguata: le reti IT o OT non adeguatamente segmentate consentono agli hacker di spostarsi da un primo punto di accesso nella rete aziendale direttamente verso i sistemi operativi o tra sistemi IT critici. Inoltre, l'intelligenza artificiale viene oggi utilizzata per combinare diverse vulnerabilità che, in passato, avrebbero limitato la capacità degli attaccanti di muoversi all'interno delle reti, rendendo ancora più fondamentale una vera e propria segmentazione dei dati.



Esposizione a terze parti: fornitori, Managed Service Provider (MSP) e piattaforme software rappresentano importanti vettori di accesso iniziale. Gli attori malevoli arrivano a prendere di mira anche le terze parti dei fornitori per raggiungere ambienti particolarmente interessanti e strategici.



Lacune nel rilevamento e nella risposta: un monitoraggio insufficiente delle attività anomale, una capacità limitata di contenere rapidamente gli incidenti e piani di continuità operativa e risposta non testati o non adeguatamente collegati ai servizi critici dell'organizzazione possono amplificare significativamente le conseguenze di un attacco. Poiché l'AI consente agli attaccanti di accelerare alcune fasi della sequenza di attacco, l'impatto di queste lacune potrebbe diventare ancora più significativo.

Queste criticità presentano uno schema ricorrente. In quasi tutti i casi di cui Control Risks si è occupato, l'organizzazione non ha individuato l'intrusione in tempo, non è riuscita a contenerla una volta che ha iniziato a diffondersi, non era in grado di continuare a operare senza il sistema compromesso e non si era preparata adeguatamente a gestire nessuno di questi scenari.

28 Verizon, Rapporto sulle indagini relative alle violazioni dei dati 2025: lo sfruttamento delle vulnerabilità come vettore di accesso iniziale è aumentato del 34% rispetto all'anno precedente ed è stato riscontrato nel 20% delle violazioni; si trattava prevalentemente di problemi noti e risolvibili tramite patch nei dispositivi periferici e nelle VPN. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

29 https://www.crowdstrike.com/en-us/global-threat-report/

Secondo l'esperienza di Control Risks, sono proprio queste carenze a fare la differenza tra un incidente circoscritto e una crisi aziendale:

Figura 6: Perché gli incidenti si trasformano in crisi

La criticità	Come si manifesta	Perché l'incidente si aggrava
Non sono riusciti a rilevarlo	Copertura del monitoraggio parziale; alert non verificati al di fuori dell'orario di lavoro	Gli hacker ora riescono a muoversi in modo laterale in circa 30 minuti;[30] un accesso non rilevato può portare alla compromissione dell'intero ambiente
Non sono riusciti a contenerlo	Reti non segmentate, credenziali condivise, accessi privilegiati permanenti	Un primo punto di accesso alla rete aziendale consente agli attaccanti di raggiungere i sistemi operativi e di produzione
Non erano in grado di operare senza il sistema colpito	I servizi critici non sono stati mappati rispetto ai sistemi e ai fornitori da cui dipendono	Un'interruzione tecnica si traduce in perdite di fatturato; i tempi di inattività causati dal ransomware si aggirano ora in media intorno ai 24 giorni[31]
Non si erano preparati adeguatamente	Piani predisposti ma mai testati, né sperimentati al di fuori del team tecnico	Le decisioni a livello dirigenziale vengono prese per la prima volta proprio nel momento di massima pressione

Fonte: Casi di risposta agli incidenti gestiti da Control Risks.

30 https://www.crowdstrike.com/en-us/global-threat-report/
31 Rapporto trimestrale di Coveware by Veeam sul ransomware e relativa analisi di settore, 2025.

Le funzioni aziendali sono di per sé delle superfici di attacco

Gli hacker non prendono di mira le organizzazioni in modo casuale. Anche i gruppi più opportunistici seguono strategie, preferenze e percorsi di minore resistenza, individuando dove si trovano le opportunità di compromissione più semplici. Prendono di mira le funzioni che gestiscono accessi, denaro, dati o relazioni di fiducia, perché rappresentano la via più rapida per provocare un'interruzione e offrono la maggiore leva estorsiva per colpire l'organizzazione nel suo complesso.

Nei casi gestiti da Control Risks, le funzioni riportate di seguito sono quelle più frequentemente prese di mira come vettore iniziale di accesso alle organizzazioni, e non sempre sono quelle che le organizzazioni si aspetterebbero:



IT, sicurezza e amministratori con accessi privilegiati: il furto di credenziali e il furto d'identità nel servizio di assistenza possono trasformare una singola compromissione in un incidente esteso all'intera organizzazione.



Finanza, paghe e procurement: il potere di autorizzare i pagamenti rende queste funzioni obiettivi allettanti per attacchi di tipo "business email compromise", frodi sulle fatture e dirottamento dei pagamenti tramite deepfake.



Operations, engineering e OT: sono le aree in cui un'interruzione digitale può tradursi in conseguenze fisiche e i tempi di fermo possono generare costi operativi significativi.



Funzioni commerciali e di vendita: la loro esposizione verso l'esterno può trasformarle in un punto di accesso ai dati e ai sistemi dei clienti.



Dirigenza e consiglio di amministrazione: dispongono di poteri decisionali e autorizzativi e rappresentano quindi bersagli privilegiati per i tentativi di impersonificazione.



Risorse umane e gestione del personale: gestiscono dati personali e candidature provenienti dall'esterno, con una conseguente esposizione a tecniche come l'infiltrazione di falsi professionisti IT.

Alcuni ruoli sono oggetto di attacchi con una frequenza significativamente superiore rispetto ad altri. Il personale che si occupa di fusioni e acquisizioni (M&A) e chi ricopre ruoli strettamente legati alla negoziazione di operazioni, alle cessioni e agli investimenti rappresenta un bersaglio particolarmente rilevante sia per gli attori mossi da motivazioni finanziarie sia per quelli interessati a ottenere vantaggi commerciali.

Secondo le ricerche di Control Risks e l'esperienza maturata con i clienti del settore privato, circa il 18% del totale delle vittime di ransomware e di estorsioni basate sulla sottrazione e diffusione di dati era stato coinvolto in un'operazione pubblica di fusione o acquisizione nei 12 mesi precedenti. Il dato suggerisce una particolare esposizione delle organizzazioni coinvolte in operazioni di M&A rese pubbliche. Nelle aziende del comparto privato, il personale che si occupa di fusioni e acquisizioni è spesso bersaglio di tentativi di phishing e di social engineering, più frequentemente rispetto ai team IT o a quelli Finance interni. Questa tendenza si riscontra in diversi settori, con una particolare esposizione del personale M&A anche in comparti diversi dai mercati dei capitali.

Le funzioni aziendali possono aumentare l'esposizione e rendere più complessa la resilienza in tre aree principali:

Targeting diretto:
come detto prima, gli autori delle minacce prendono di mira specifiche funzioni aziendali all'interno delle organizzazioni utilizzando una serie di tecniche di social engineering per compromettere i sistemi, causare interruzioni, rubare dati o ricattare.

Gestione delle vulnerabilità:
carenze nell'individuazione di software non autorizzati, compresi strumenti di AI utilizzati senza approvazione, nell'aggiornamento dei sistemi legacy e nell'applicazione uniforme dei controlli di sicurezza sui diversi dispositivi possono creare vulnerabilità facilmente sfruttabili dagli attaccanti.

Pianificazione inadeguata della resilienza:
sebbene i sistemi e le tecnologie siano sempre più gestiti in modo centralizzato, le diverse esigenze delle singole funzioni aziendali in termini di continuità operativa, dipendenze e ridondanza non sempre trovano adeguato riscontro nella pianificazione della resilienza, aumentando così il potenziale costo di un'interruzione.

Cinque consigli per rafforzare la resilienza operativa e ridurre i tempi di ripristino

La resilienza non è semplicemente una condizione da raggiungere o un indicatore del livello di maturità di un'organizzazione. Dall'analisi condotta da Control Risks emerge che le organizzazioni che riescono a riprendersi rapidamente tendono ad aver adottato un numero ristretto di misure ricorrenti, nessuna delle quali richiede necessariamente nuove tecnologie. Ciò che serve è piuttosto una chiara responsabilità nell'individuare ciò di cui l'organizzazione non può fare a meno per continuare a operare, e la capacità di riesaminare costantemente questa valutazione man mano che dipendenze ed esigenze evolvono.

Figura 7: Cinque attività chiave per la resilienza che influenzano i tempi di ripristino



1 **Sicurezza proattiva**	Implementare l'autenticazione a più fattori (MFA) ovunque sia tecnicamente possibile, eliminare gli accessi privilegiati permanenti, risolvere prima le vulnerabilità note e già sfruttate e separare le reti IT da quelle OT in modo che un accesso alla rete aziendale non consenta di raggiungere i sistemi di produzione.
2 **Governance e responsabilità**	Valutare il profilo di rischio, concordare la propensione al rischio con i principali stakeholder e nominare un unico responsabile per la gestione delle dipendenze e della continuità operativa. Quando questa responsabilità si colloca a cavallo tra sicurezza, procurement e business continuity, il rischio è che nessuno ne abbia realmente la responsabilità.
3 **Mappatura delle dipendenze**	Mappare i servizi critici rispetto ai sistemi, ai fornitori e ai subfornitori sottostanti, individuare i casi in cui il ripristino richiede il coinvolgimento di terze parti, concordare soluzioni alternative e definire, ove possibile, le aspettative contrattuali in materia di ripristino, nonché le priorità e le alternative praticabili.
4 **Test ed esercitazioni**	Testare le capacità di ripristino considerando non soltanto l'indisponibilità di un sistema, ma anche quella di un provider, coinvolgendo nelle esercitazioni sia il management sia i team tecnici. Un piano mai testato si basa su presupposti, e sono proprio i presupposti a venire meno per primi.
5 **Preparazione e risposta**	Assicurarsi preventivamente la disponibilità di competenze e risorse in ambito forense, legale e comunicazione; esercitarsi sui criteri e sulle soglie che guidano il processo decisionale e rivalutare periodicamente il profilo di rischio man mano che evolvono l'infrastruttura tecnologica e la base dei fornitori. Preparare queste decisioni in anticipo riduce il numero di scelte che devono essere affrontate per la prima volta durante una crisi, favorendo un ripristino più rapido e limitando l'impatto sull'operatività.

Fonte: Control Risks

Nel loro insieme, queste cinque attività consentono di rispondere a quattro domande fondamentali, a cui ogni organizzazione dovrebbe essere in grado di rispondere con dati concreti.

- → È in grado di individuare un'intrusione abbastanza tempestivamente da poter intervenire?
- → È in grado di contenere l'intrusione prima che raggiunga i sistemi operativi?
- → È in grado di continuare a fornire i suoi servizi più importanti anche quando il sistema colpito non è disponibile?
- → Ha testato concretamente la propria capacità di farlo, coinvolgendo sia il management sia i team tecnici?

Le organizzazioni che riescono a rispondere a tutte e quattro le domande tendono a riprendersi più in fretta. Quelle che non ci riescono hanno meno controllo sulla durata e sull'impatto delle interruzioni, soprattutto quando la ripresa dipende da terzi. È per questo che la gestione delle dipendenze è una questione che deve arrivare all'attenzione del board: incide sui tempi di ripristino, sul costo effettivo dell'interruzione e sulla misura in cui la continuità operativa dell'organizzazione dipende da soggetti esterni al proprio perimetro.

Al cuore del rischio: il punto di vista dei nostri underwriter



Stefano Pompeo
Cyber Senior Underwriter QBE Italia

Uno degli insegnamenti più evidenti che emerge dai sinistri cyber che osserviamo è che la gravità di un incidente non dipende necessariamente dalla sofisticatezza dell'attacco. Spesso, ciò che conta di più è quello che succede dopo: quanto si propaga l'interruzione all'interno dell'organizzazione, quali servizi critici diventano indisponibili, quanto rapidamente possono essere ripristinati e in che misura il ripristino dipende da terze parti. Tutto questo cambia il modo in cui noi, e le aziende stesse, dovremmo considerare la resilienza informatica.

Solidi controlli di sicurezza restano fondamentali, ma pensare di poter prevenire ogni incidente non è realistico. Le organizzazioni devono anche comprendere come potrebbero continuare a operare qualora un sistema critico, un fornitore o una piattaforma tecnologica diventassero indisponibili e quanto controllo abbiano effettivamente sui propri tempi di ripristino.

Per gli underwriter, si tratta di una distinzione importante e significativa. Due aziende con misure di sicurezza informatica apparentemente simili possono avere livelli di esposizione al rischio molto diversi. Una potrebbe aver mappato i servizi critici, segmentato le reti, testato i backup, individuato fornitori alternativi e svolto esercitazioni coinvolgendo il senior management. Un'altra potrebbe scoprire le proprie dipendenze critiche soltanto dopo che si è verificato un incidente. L'evento cyber iniziale potrebbe essere simile, ma le conseguenti interruzioni dell'attività molto diverse.

Questo aspetto assume particolare rilevanza man mano che le organizzazioni dipendono sempre di più da un numero relativamente ristretto di fornitori di tecnologia. Servizi gestiti, piattaforme e sistemi hanno generato enormi efficienze, ma possono anche creare delicati punti di dipendenza comuni.

Le aziende devono quindi guardare oltre la tradizionale gestione dei rischi legati alle terze parti. Non basta più sapere chi sono i propri fornitori diretti. Occorre porsi una domanda fondamentale: chi altro deve essere operativo affinché possiamo continuare a esserlo noi? La risposta potrebbe includere il provider cloud di un fornitore, una piattaforma software o un altro subappaltatore; qualcuno con cui la propria organizzazione non ha alcun rapporto diretto. E se quel provider diventa indisponibile, anche i tempi di ripristino dell'azienda possono finire per dipendere da soggetti esterni.

È anche per questo che il rischio di concentrazione assume un'importanza crescente. Le singole imprese non possono, da sole, diversificare un mercato in cui tantissime organizzazioni dipendono dagli stessi fornitori critici. Autorità di regolamentazione e governi hanno quindi un ruolo importante nell'individuare e gestire le dipendenze tecnologiche sistemiche, parallelamente alle responsabilità delle singole organizzazioni.

Il ripristino deve essere pianificato, non dato per scontato

Uno degli esercizi più utili che un'azienda possa fare è partire dai propri servizi critici e procedere a ritroso.

Cosa deve continuare a funzionare? Quali sistemi e fornitori lo rendono possibile? Per quanto tempo l'azienda potrebbe andare avanti senza di essi? Quali sono le alternative? Chi ha l'autorità per prendere decisioni quando si verifica un'interruzione?

A queste domande bisognerebbe rispondere prima che si verifichi un incidente, non mentre è in corso.

Altrettanto importante è testare quanto pianificato. Un piano di risposta agli incidenti può sembrare completo sulla carta, ma basarsi su presupposti che non sono mai stati messi alla prova. Consigliamo alle organizzazioni di effettuare anche degli "stress test" per simulare la perdita di un fornitore o l'indisponibilità di un sistema interno, coinvolgendo in queste esercitazioni i responsabili delle decisioni a livello dirigenziale insieme ai team di sicurezza informatica e IT. Le aziende dovrebbero stabilire e pianificare in anticipo quando attivare le misure di continuità operativa, comunicare con i clienti, coinvolgere specialisti esterni o assumere altre decisioni critiche. Il livello di preparazione può influire in modo significativo sull'entità di una perdita. L'obiettivo non si limita al ripristino della tecnologia: l'attenzione dovrebbe concentrarsi sul mantenimento della capacità di fornire i servizi più importanti mentre sono in corso le attività di ripristino.

Non trascurare le imprese di minori dimensioni

C'è poi una sfida importante per i governi, le compagnie assicurative e tutto il settore della sicurezza informatica, che riguarda le piccole e medie imprese (PMI). Le grandi organizzazioni sono sottoposte a pressioni normative e commerciali che le spingono a dimostrare la propria resilienza informatica, mentre le PMI spesso hanno meno risorse interne, pur facendo affidamento su molte delle stesse tecnologie e su filiere interconnesse.

È fondamentale aumentare la consapevolezza e offrire un sostegno concreto a queste realtà. La resilienza informatica non richiede per forza tecnologie sofisticate o costose. Misure ragionevoli come l'autenticazione a più fattori (MFA), l'eliminazione degli accessi privilegiati non necessari, l'applicazione di patch alle vulnerabilità sfruttate, il mantenimento di backup efficaci e la comprensione delle dipendenze critiche dei fornitori possono già migliorare significativamente la capacità di resistere di fronte a un incidente.

Per le organizzazioni più grandi, questo rappresenta anche un tema di resilienza della supply chain. Aiutare i fornitori più piccoli a migliorare la loro resilienza può, in definitiva, proteggere la continuità delle attività che dipendono da essi.

Valorizzare le competenze a disposizione

Infine, le aziende non dovrebbero considerare l'assicurazione contro i rischi informatici esclusivamente come uno strumento finanziario che interviene a seguito di un sinistro. La relazione assicurativa può offrire accesso a competenze specialistiche prima, durante e dopo un incidente. I broker e le compagnie possono aiutare le organizzazioni a capire a quali rischi sono esposte, a individuare le aree in cui sarebbe utile pianificare la resilienza e a sfruttare al meglio i servizi specialistici a loro disposizione.

Quando si verifica un incidente, sapere in anticipo a chi rivolgersi (esperti forensi, consulenti legali, esperti di comunicazione, professionisti nella gestione degli incidenti) può far risparmiare tempo prezioso nelle prime fasi di un'emergenza.

Ambito di applicazione e note

Mercati interessati (14)

L'analisi riguarda 14 mercati in cui opera QBE:
Regno Unito, Svezia, Danimarca, Francia, Germania, Spagna, Italia, Paesi Bassi, Canada, Stati Uniti, Australia, Nuova Zelanda, Singapore e Hong Kong.

Periodo

2023-2026, con previsioni per il 2027.

Fonti e metodologia

L'analisi si basa sui dati relativi a incidenti, informazioni e interventi raccolti da Control Risks nei 14 mercati oggetto dello studio, integrati, ove indicato, da informazioni provenienti da fonti aperte e da dati di mercato forniti da terze parti.
I dati relativi al 2026 si basano sui valori registrati dall'inizio dell'anno e su una proiezione fino alla fine dell'anno; quelli relativi al 2027 sono invece previsioni elaborate sulla base della crescita media.

Metodologia dei dati

Il dataset di Control Risks si basa su informazioni selezionate per un pubblico corporate, tipicamente costituito da grandi multinazionali, e si concentra sugli incidenti di rilevanza strategica. Questo approccio differisce da quello dei provider che raccolgono dati attraverso strumenti di Endpoint Detection and Response (EDR) implementati presso la propria base clienti e che, pertanto, rilevano generalmente incidenti riguardanti sia grandi multinazionali sia imprese di minori dimensioni.

I dati di Control Risks non comprendono necessariamente tutti gli incidenti che potrebbero essere rilevati da uno strumento automatizzato, ma offrono una rappresentazione significativa degli incidenti che interessano le grandi aziende nei mercati presi in esame.



Per maggiori informazioni su questo report, visita **qbeitalia.com** o contattaci scrivendo a **qbemilan@it.qbe.com**

QBE European Operations
QBE Europe SA/NV
Rappresentanza Generale per l'Italia
Via Melchiorre Gioia 8
20124 Milano
Italy
+39 02 3626 3500

QBEitalia.com

Il presente report è stato realizzato da QBE in collaborazione con Control Risks.

Tutti i prodotti e i servizi sono forniti da QBE Insurance Group Limited o dalle sue società controllate ("QBE"), oppure da fornitori terzi selezionati da QBE, e possono essere soggetti a ulteriori termini e condizioni, limitazioni ed esclusioni di responsabilità [disponibili su richiesta]. Le informazioni e le indicazioni fornite da QBE non costituiscono una consulenza finanziaria o professionale personalizzata in base alle specifiche circostanze del destinatario e potrebbero non essere state elaborate sulla base di una conoscenza approfondita dei suoi sistemi o dei rischi a cui è esposta la sua attività. Inoltre, non contemplano tutte le possibili situazioni o azioni che potrebbero rendersi necessarie per rispondere a un incidente di sicurezza informatica. QBE non fornisce alcuna garanzia in merito ai risultati, ad esempio in termini di riduzione dell'esposizione ai sinistri, né garantisce che un prodotto o servizio risponda alle specifiche esigenze del destinatario. Spetta al destinatario valutare autonomamente le indicazioni fornite e l'idoneità di qualsiasi prodotto. Tali indicazioni non sostituiscono la consulenza di professionisti legali o esperti di sicurezza informatica nella preparazione o nella risposta a un incidente di sicurezza informatica. QBE non è responsabile dei servizi forniti dai propri fornitori terzi. QBE e il logo utilizzato sono marchi registrati di QBE Insurance Group Limited; i marchi di terzi sono utilizzati sulla base delle relative licenze. © 2026 QBE Insurance Group Limited.

QBE European Operations è un nome commerciale di QBE Europe SA/NV, QBE UK Limited e QBE Underwriting Limited. QBE Europe SA/NV, P.IVA BE 0690.537.456, RPM/RPR Bruxelles, è autorizzata dalla Banca Nazionale del Belgio con licenza numero 3093. QBE UK Limited e QBE Underwriting Limited sono autorizzate da Prudential Regulation Authority e regulate da Financial Conduct Authority e Prudential Regulation Authority.

1475304/2611-IT

QBE Insurance