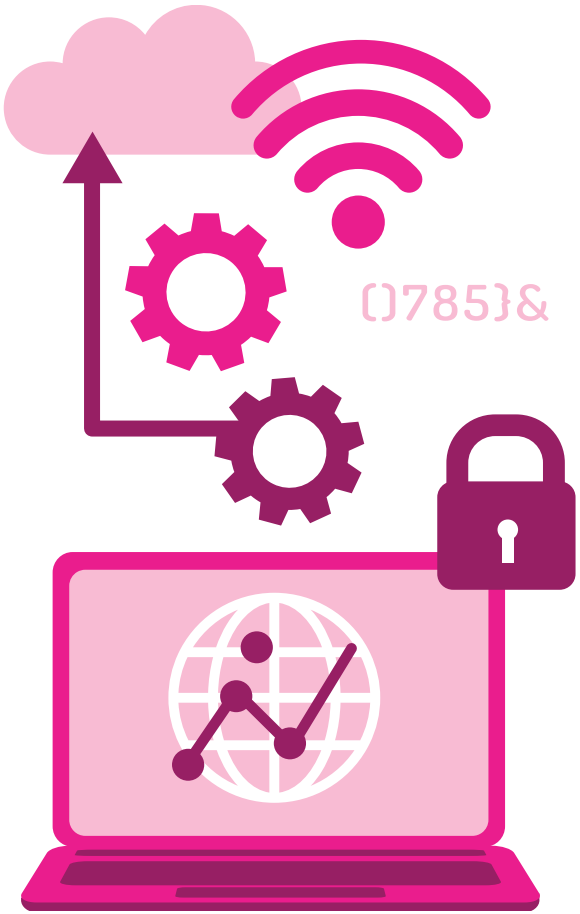
CHUBB®

# Guida pratica per i broker al Cyber Risk Management

# Questa guida include informazioni relative a:

# Perché è importante il Cyber?



## L'era informatica e digitale ci consente di raccogliere sempre più dati, collaborare in modo sempre più efficiente, snellire sempre più i processi aziendali ed estrarre informazioni in tutto il mondo 24 ore su 24, 7 giorni su 7.

**L'aumento della dipendenza dai sistemi informatici e dall'accesso ai dati accrescono significativamente la vulnerabilità di un'azienda alle minacce legate alla sicurezza informatica.** Interruzioni, errori o attacchi a questi nuovi processi possono comportare significativi costi extra, in grado di compromettere i risultati economici di un'azienda. Pertanto, quando accadrà, sarà necessaria una protezione completa da parte di un assicuratore specializzato nella gestione dei rischi cyber, in grado di offrire un pacchetto completo di soluzioni assicurative integrate per minimizzare eventuali gap di copertura e capace di adattare la copertura offerta alla attività svolta. **Chubb fornisce ai propri assicurati soluzioni ai rischi cyber sin dal 1998.**

### Lacune nelle assicurazioni tradizionali

Le aziende spesso operano nella convinzione che le proprie polizze assicurative esistenti siano sufficienti a coprire le proprie esposizioni legate alla sicurezza dei dati e alla privacy. Sfortunatamente non sempre è così e le polizze assicurative tradizionali potrebbero non essere adeguate a mitigare le esposizioni che le aziende sono chiamate ad affrontare oggi.
Si considerino le seguenti polizze tradizionali:

| Responsabilità civile generale | Property | Crime |
|---|---|---|
| Di norma, le polizze di responsabilità civile generale si attivano in risposta a richieste di risarcimento per danni a cose o danni a persone. Un evento cyber solitamente non comporta né danni a cose né danni a persone e, in genere, le polizze di responsabilità civile generale non offrono copertura per i danni propri sofferti dalla contraente. | Le polizze property tipicamente rispondono alla distruzione o al danneggiamento di beni tangibili derivanti da un danno materiale. La perdita tangibile, di conseguenza, permette l'attivazione delle garanzie di interruzione dell'attività e spese extra. Un evento cyber, di per sé, non comporta danni materiali, tuttavia può costringere un'impresa all'interruzione dell'attività con conseguenti costi e spese rilevanti e perdita di profitto. | Le polizze crime tipicamente rispondono a danni diretti derivanti dal furto di denaro, titoli o proprietà tangibili da parte dei propri dipendenti. L'estensione Computer Crime solitamente esclude la responsabilità verso terze parti e potrebbe non offrire sufficiente copertura nei casi di perdita di dati sensibili. |

# Esposizione al rischio per settore

## Istituzioni finanziarie

Le istituzioni finanziarie sono fortemente esposte al rischio cyber a causa di una combinazione di fattori. Il cybercrime, l'hacktivismo e gli hacker più sofisticati che svolgono attività di spionaggio per conto di un terzo beneficiario rappresentano solo alcuni dei rischi da considerare. Le vulnerabilità agli eventi cyber possono essere elevate per molte istituzioni finanziarie, considerata la dipendenza dei loro sistemi da reti altamente interconnesse e da infrastrutture critiche. A causa di un'elevata dipendenza dalla tecnologia, l'esposizione al rischio cyber per la maggior parte delle istituzioni finanziarie continuerà a crescere.

Esempi di sinistri:
**Phishing** ed
**Errore umano**

## Settore sanitario

L'avvento della digitalizzazione delle cartelle cliniche ha prodotto una maggiore dipendenza delle aziende sanitarie dai sistemi informatici per la raccolta e il trattamento dei dati sanitari e medici altamente sensibili. Vi è un'elevata esposizione ad errori amministrativi poiché, per l'inserimento nei sistemi di informazioni corrette, si fa affidamento sui dipendenti.I sistemi informatici obsoleti sono spesso non segregati e ciò aumenta il rischio che un singolo evento possa avere un notevole impatto sulle operazioni.

Esempi di sinistri:
**Errore umano**
e **Uso improprio**

## Commercio al dettaglio

Sia in relazione ai canali di vendita online sia presso i negozi fisici, i dati sui sinistri gestiti da Chubb mostrano che il settore del commercio al dettaglio è significativamente esposto agli eventi cyber. Le aziende operanti nel settore del commercio al dettaglio sono spesso caratterizzate da un elevato numero di sedi che non sempre operano su sistemi IT centralizzati, dalla dipendenza da una complessa rete di fornitori di servizi IT critici, da una potenziale dipendenza dai siti web legata al crescente numero di vendite online e da una elevata aggregazione di dati personali sensibili dovuta all'alta frequenza di transazioni finanziarie e a programmi di fidelizzazione.

Esempi di sinistri:
**Attacchi hacker**
e **Phishing**

## Settore alberghiero

Il settore alberghiero copre una vasta gamma di attività tra cui hotel, bar e ristoranti. Trasversalmente a tutto il settore, le principali esposizioni cyber sono legate agli ingenti volumi di dati relativi a consumatori e dipendenti, alla spesso massiccia dipendenza dall'utilizzo di siti web per le prenotazioni e all'elevato numero di dati processati tramite programmi fedeltà che possono comportare problemi di privacy, rappresentando un bersaglio per attacchi di phishing ed ingegneria sociale.

Esempi di sinistri:
**Phishing** e
**Attacchi hacker**

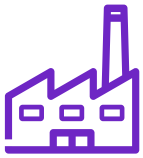
## Servizi professionali

A causa della quantità di dati sensibili raccolti, il settore dei servizi professionali è un obiettivo comune per gli attacchi informatici. Per esempio, i dati sensibili detenuti da uno studio legale o da un commercialista possono essere redditizi per un hacker e questo può produrre gravi conseguenze reputazionali per uno studio professionale che subisce una tale violazione. Negli ultimi anni, l'aggregazione di informazioni sensibili relative ai propri clienti ha determinato un incremento degli eventi cyber che hanno avuto un impatto sulle società che erogano servizi professionali.

Esempi di sinistri:
**Errore umano**
e **Attacchi hacker**

* Cause comuni di sinistri cyber che provengono dal Chubb Cyber Index®

# Esposizione al rischio per settore



## Industria manifatturiera

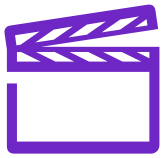
L'industria manifatturiera rappresenta uno dei principali settori presi di mira dai cyber criminali. L'aumento dell'integrazione tecnologica sta cambiando il modo in cui i produttori gestiscono le loro attività. Al fine di migliorare la produttività e l'efficienza dei costi, molti produttori stanno implementando l'Internet delle cose (IoT - Internet of Things),la digitalizzazione e i servizi cloud, aumentando l'esposizione al rischio cyber. I recenti eventi che hanno impattato i Sistemi di controllo industriale (ICS - Industrial Control Systems) e i Sistemi di supervisione controllo e acquisizione dati (SCADA - Supervisory Control And Data Acquisition) hanno paralizzato l'intera operatività aziendale.

Esempi di sinistri:
**Malware** e **Phishing**

## Istruzione

La principale esposizione degli istituti scolastici è legata ai dati sensibili di studenti e personale di cui sono in possesso. Le scuole e le università hanno spesso budget e risorse IT limitati. Le minacce possono essere sia esterne sia interne, che si tratti di uno studente che introduce un malware all'interno della rete intenzionalmente o inavvertitamente, o di un membro dello staff che non rispetta il protocollo, causando una violazione dei dati.

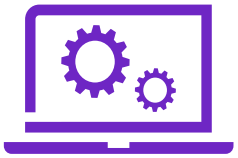
Esempi di sinistri:
**Phishing** e **Attacchi hacker**



## Media/Intrattenimento

Le società nel settore media e intrattenimento spesso devono affrontare minacce di cyber estorsione che hanno come bersaglio materiale e contenuti sensibili. Gli attacchi distribuiti di Denial of Service (DDoS - negazione del servizio) o le interruzioni di operatività dei sistemi informatici possono avere un impatto significativo sulle attività di trasmissione e sulla consegna tempestiva dei contenuti. Il possesso di dati personali sensibili degli abbonati comporta un'ulteriore esposizione al rischio.

Esempi di sinistri:
**Errore umano** e **Phishing**



## Servizi informatici

I clienti ripongono la massima fiducia nelle aziende informatiche, considerandole quali leader del settore nella sicurezza informatica e nella protezione dei dati; di conseguenza, un potenziale evento cyber aumenterebbe esponenzialmente il danno alla reputazione che ne potrebbe derivare. Gli eventi cyber a danno dei fornitori di servizi informatici possono impattare anche la copertura di Responsabilità Civile Professionale degli stessi fornitori. Rivolgiti al tuo assuntore in Chubb per avere ulteriori informazioni sulla nostra offerta assicurativa relativa ai prodotti Cyber ed RC Professionale per società informatiche.

Esempi di sinistri:
**Attacchi hacker** e **Errore umano**

*Cause comuni di sinistri cyber che provengono dal Chubb Cyber Index®

**Scopri l'offerta di Chubb per le piccole, medie e grandi imprese per mitigare queste esposizioni:**

**Piccole imprese** | **Medie imprese** | **Grandi imprese**

# Piccole imprese - Panoramica

Sebbene l'attenzione dei media si concentri prevalentemente sugli eventi cyber subiti dalle grandi aziende, le PMI sono spesso colpite da minacce e vulnerabilità informatiche. Le piccole imprese sono spesso considerate obiettivi più semplici per i cyber criminali, a causa di risorse e investimenti IT spesso limitati.

Inoltre, potrebbero essere maggiormente inclini a trascurare misure quali la formazione del personale sulla sicurezza dei dati, la guida sull'impostazione delle password e l'autenticazione a due fattori. Le PMI rappresentano spesso un'opportunità di lucro per i cyber criminali rispetto alle aziende più grandi, che potrebbero risultare più difficili da attaccare. Esiste anche il caso in cui le PMI potrebbero non rappresentare l'obiettivo iniziale dell'attacco, ma subire un impatto indiretto a seguito di un evento cyber che ha colpito il proprio fornitore IT o il proprio partner commerciale.

## Sinistri delle piccole imprese - Chubb Cyber Index®

Il modo migliore per illustrare il rischio cyber a cui le piccole imprese vanno incontro è attraverso i dati. Chubb gestisce i sinistri cyber da oltre vent'anni. Come parte integrante del processo di gestione dei sinistri, monitoriamo i parametri chiave come le azioni che causano un evento cyber, sia esso di origine interna o esterna, il numero di dati impattati, le dimensioni e il settore degli assicurati interessati. Attraverso il Chubb Cyber Index®, condividiamo pubblicamente questi dati per aiutare le aziende a comprendere meglio i rischi che affrontano.

Il Chubb Cyber Index® fornisce agli utenti uno strumento utile ad identificare i principali rischi cyber che la loro azienda potrebbe dover affrontare sulla base di esempi reali di attacchi informatici e violazioni dei dati. Gli utenti possono impostare i parametri e visualizzare i trend storici in base al tipo di minaccia, alle dimensioni dell'azienda e al settore in cui opera.

Per ulteriori informazioni, visita il Chubb Cyber Index® su: **https://chubbcyberindex.com**

# Piccole imprese - Scenari di sinistro

## Ransomware

Il nostro assicurato, una società di costruzioni, è stato vittima di un attacco ransomware mirato. I sistemi dell'assicurato sono stati violati dopo che un dipendente ha fatto clic su un collegamento dannoso contenuto in un'e-mail. I sistemi e i server dell'assicurato sono stati crittografati e successivamente è comparsa una richiesta di 800.000 sterline in bitcoin. L'assicurato ha consultato gli Incident Response manager di Chubb al fine di istruire gli esperti di informatica forense per stabilire il metodo e la portata dell'attacco. Pur non avendo pagato il riscatto, le operazioni commerciali complessive sono state interrotte per oltre sei mesi.

**Sezione di copertura applicabile:**

Recupero di dati e sistemi, Interruzione dell'attività, Spese di incident response e Cyber estorsione.

**Attenuazione**

Revisione periodica della sicurezza IT, formazione dei dipendenti, backup periodico dei dati e attuazione di piani di Disaster Recovery e Business Continuity.

## Condotta impropria del dipendente

Il nostro assicurato è stato vittima di un dipendente disonesto che si è appropriato di oltre 700 documenti relativi a dati personali dei clienti, inclusi nomi, indirizzi e recapiti. Tali documenti sono stati forniti al nuovo datore di lavoro in favore di quest'ultimo. Poiché l'evento si è verificato in seguito all'entrata in vigore del GDPR, è stato necessario comunicarlo all'ufficio di regolamentazione locale e ai soggetti interessati.

**Sezione di copertura applicabile:**

Responsabilità derivante da violazioni di obblighi di riservatezza e Spese di incident response.

**Attenuazione**

È incredibilmente difficile impedire che dipendenti disonesti possano provare a causare danni. Molto spesso hanno accesso al sistema necessario per consentire il furto di dati sensibili personali o aziendali. In base alla giurisprudenza attuale, è probabile che una società sia responsabile nei confronti dei propri clienti. Una soluzione assicurativa cyber di Chubb fornisce gli strumenti necessari per sopperire al verificarsi di una suddetta circostanza.

## Errore di un dipendente

Il nostro assicurato, una cooperativa edilizia regionale nel Regno Unito, inavvertitamente ha subito una violazione dei dati a seguito dell'errore di un dipendente. Pubblicando un nuovo annuncio per una proprietà vacante, il dipendente ha erroneamente incluso un'immagine della documentazione medica di un altro cliente all'interno della brochure online della proprietà.

**Sezione di copertura applicabile:**

Responsabilità derivante da violazioni di obblighi di riservatezza e Spese di incident response.

**Attenuazione**

È importante disporre di una politica sulla privacy a livello aziendale che descriva il protocollo per la gestione delle informazioni sensibili. I dipendenti dovrebbero avere la responsabilità di comprendere e riconoscere la conformità della politica almeno una volta l'anno.

# Piccole imprese - Scenari di sinistro

## Accesso non autorizzato - Phishing

Il nostro assicurato, un'azienda di logistica, è stato vittima di un attacco malware di phishing. Un dipendente all'interno del team HR dell'assicurato ha cliccato su un collegamento dannoso contenuto in un'e-mail. Sul suo computer è apparso un pop-up in cui si comunicava che il computer era stato infettato e si suggeriva di contattare il numero fornito. I truffatori hanno quindi ottenuto l'accesso remoto al computer del dipendente ingannandolo ulteriormente durante la chiamata.

**Sezione di copertura applicabile:**

Responsabilità derivante da violazioni di obblighi di riservatezza, Responsabilità derivante da violazioni della sicurezza della rete e Spese di incident response.

**Attenuazione**

Anche con i migliori sistemi e tecnologie di sicurezza, la risorsa più vulnerabile di un assicurato è spesso il suo personale. Il personale può essere indotto a fornire password o accesso. Si consiglia una regolare formazione sul phishing ed è fondamentale possedere una polizza assicurativa adeguata.

## Perdita di documenti fisici

Il nostro assicurato, uno studio legale, ha contattato la incident response hotline di Chubb quando è emerso che un dipendente dello studio, infrangendo il protocollo aziendale, aveva prelevato la documentazione dei clienti dall'ufficio conservandola nella propria auto. Successivamente l'auto è stata rubata e la documentazione dei clienti smarrita.

**Sezione di copertura applicabile:**

Responsabilità derivante da violazioni di obblighi di riservatezza e Spese di incident response.

**Attenuazione**

Disporre di un processo chiaro per l'archiviazione sia fisica sia digitale dei dati. È importante effettuare il regolare backup dei dati per essere in grado di recuperarli rapidamente. Creare una politica sulla privacy a livello aziendale che i dipendenti sono tenuti a riconoscere e a rispettare.

# Piccole imprese - Una soluzione informatica su misura che cresce con te

## 1 Servizi di Loss Mitigation per piccole imprese

Per aiutare le PMI nostre assicurate a mitigare la propria esposizione al rischio cyber, Chubb offre loro numerosi servizi attraverso specifici fornitori, ove consentito dalla legge.

**Soluzioni di gestione delle password** per un massimo di 500 dipendenti di ciascun assicurato.

- Una gestione efficace delle password può aiutare a minimizzare l'utilizzo non autorizzato di credenziali rubate

**Soluzioni di formazione per i dipendenti**, che aiutano il team a prepararsi alle minacce di phishing, identificare i potenziali rischi informatici, proteggere i dati sensibili e segnalare i problemi alle persone giuste quando necessario.

**Clicca qui per maggiori informazioni sul nostro pacchetto completo di servizi cyber, tra cui la sicurezza informatica e altro ancora.**

## 2 Servizi di Incident Response per piccole imprese

Chubb comprende che non tutti gli eventi possono essere evitati. Quando accade qualcosa, le nostre polizze cyber mettono a disposizione un panel di esperti fornitori di servizi di Incident Response per le piccole imprese nostre clienti.

Questi specialisti sono a disposizione 24 ore su 24, 7 giorni su 7, 365 giorni all'anno e sono preparati a guidarti nella ripresa da qualsiasi evento cyber.

- I servizi offerti dagli esperti includono la gestione del processo di incident response, l'informatica forense, le risorse legali, le pubbliche relazioni e altro ancora
- L'accesso alla rete dei fornitori è incluso come parte della polizza
- Disponibili 24 ore su 24, 7 giorni su 7, 365 giorni all'anno tramite l'app Cyber Alert® di Chubb o il numero verde
- Possono fornire assistenza in seguito a qualsiasi evento cyber: sono pronti per aiutare in qualsiasi emergenza

**Qui troverai maggiori informazioni su come opera il servizio di Incident Response di Chubb.**

## 3 Piattaforme per le piccole imprese

Le piattaforme online di Chubb (disponibili in Paesi selezionati) sono state progettate appositamente per gli intermediari al fine di quotare e sottoscrivere online l'assicurazione di piccole imprese. Coniugando il design intuitivo all'esperienza incentrata sul cliente, gli intermediari possono formulare preventivi cyber per i loro clienti in pochi minuti e inviare subito la relativa documentazione.

**Costruire la copertura rapidamente, facilmente e con gli stessi vantaggi di una procedura offline:**

- Poche semplici domande
- Ampia propensione al rischio per PMI
- Stesso linguaggio della polizza cyber disponibile offline
- Accesso ai servizi di Loss Mitigation di Chubb
- Possibilità di modificare le date, i limiti, le commissioni e i recapiti della polizza senza la necessità di contattare un assuntore
- Possibilità di quotare ed emettere le polizze in pochi minuti

**Contatta il tuo assuntore Chubb locale per scoprire dove abbiamo capacità assicurative cyber online o altre soluzioni semplificate per le PMI.**

# Medie imprese - Panoramica

Le medie imprese affrontano gli stessi problemi di sicurezza informatica delle grandi imprese, ma con meno budget a disposizione e non altrettanto personale specializzato per gestire il rischio. Spesso sono dello stesso parere delle PMI, ossia pensano che solo le grandi imprese globali corrano un rischio significativo. Poiché le attività dannose sono diventate più sofisticate, la lotta delle medie imprese per difendersi è ora più difficile che mai.

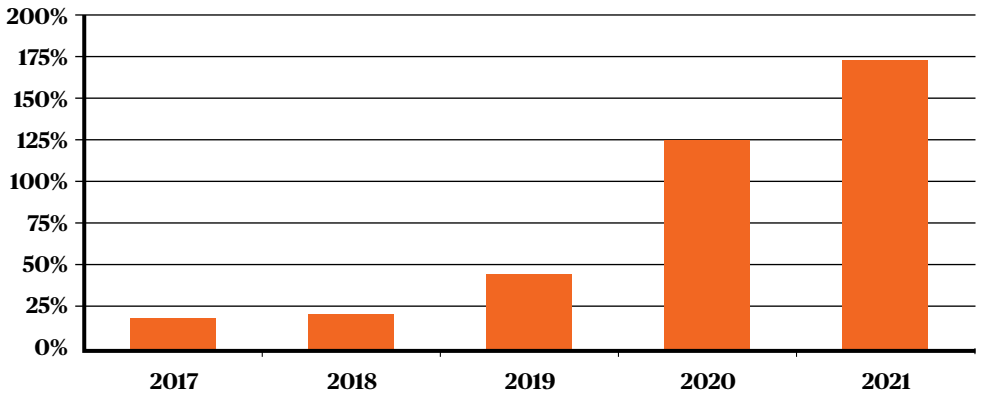
**Chubb Cyber Index®**

Il Chubb Cyber Index® fornisce agli utenti uno strumento utile ad identificare i principali rischi cyber che la loro azienda potrebbe dover affrontare sulla base di esempi reali di attacchi informatici e violazioni dei dati. Gli utenti possono impostare i parametri e visualizzare i trend storici in base al tipo di minaccia, alle dimensioni dell'azienda e al settore in cui opera.

Per ulteriori informazioni, visita il Chubb Cyber Index® su:
**https://chubbcyberindex.com**

**Sinistri Chubb rispetto al 2016 (crescita percentuale)**

*Medie imprese - Tutti i settori*




# Medie imprese - Scenari di sinistro

## Ransomware

Una struttura di assistenza sanitaria ha subito un attacco ransomware di tipo “brute force” e molti dei suoi file sono stati criptati. Inizialmente era stato richiesto un riscatto di circa 26.000 euro. Dopo aver pagato una piccola parte del riscatto per ottenere un campione dello strumento di decrittazione, l’impresa ha invece deciso di contare sui propri backup per ripristinare i sistemi.

**Sezione di copertura applicabile:**

Recupero di dati e sistemi, Interruzione dell’attività, Spese di incident response e Cyber estorsione.

**Attenuazione**

Investire sulla tecnologia di sicurezza, sebbene fondamentale per aiutare a prevenire l’accesso non autorizzato, non è infallibile. Gli aggressori mutano continuamente i loro metodi di attacco e qualsiasi azienda deve rivedere regolarmente la propria sicurezza e le proprie procedure per adeguarsi alla minaccia.

## Errore di un dipendente

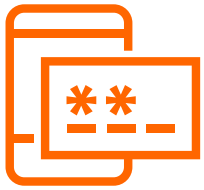
Un dipendente presso un rivenditore di hardware ha ignorato le politiche e le procedure interne e ha aperto un file apparentemente innocuo allegato a un’e-mail. Il giorno successivo, gli ordini di magazzino e i registratori di cassa del negozio di hardware hanno iniziato a dare problemi e l’attività aziendale è stata ostacolata a seguito della mancanza di rete.

**Sezione di copertura applicabile:**

Recupero di dati e sistemi, Responsabilità derivante da violazioni della sicurezza della rete, Interruzione dell’attività e Spese di incident response.

**Attenuazione**

Una formazione periodica per garantire che il personale sia in grado di riconoscere e-mail sospette e le procedure da seguire in tale circostanza. Inoltre, l’accesso immediato a un incident manager e a una rete di esperti consentirà una risposta rapida.



## Violazione dei dati

La rete di una catena alberghiera è stata hackerata compromettendo potenzialmente tutti i documenti appartenenti sia ai dipendenti sia ai clienti, tra cui le informazioni sulle carte di pagamento.

**Sezione di copertura applicabile:**

Spese di incident response, Recupero di dati e sistemi, Responsabilità derivante da violazioni di obblighi di riservatezza e Responsabilità derivante da violazioni della sicurezza della rete.

**Attenuazione**

Un sistema di rilevazione delle intrusioni (IDS - Intrusion Detection System) è uno strumento utile per contrastare gli hacker. Consente infatti di rilevare rapidamente qualsiasi attività sospetta. È inoltre fondamentale la cifratura dei dati per garantire che i dati violati sottratti non possano essere facilmente rimossi e utilizzati.

# Medie imprese - Scenari di sinistro

## Cryptomining

Un'azienda manifatturiera ha subito un attacco ransomware che ha portato alla cifratura di molti dei propri file. Dopo che l'assicurato ha contattato Chubb attraverso la incident response hotline attiva 24 ore su 24, 7 giorni su 7, abbiamo offerto la consulenza di un Incident Response manager e di esperti di informatica forense dal nostro panel. A seguito delle indagini, l'assicurato ha scelto di non pagare il riscatto. Tuttavia, una volta che l'azienda di informatica forense ha iniziato a lavorare alla risoluzione dell'attacco ransomware, ha scoperto che l'assicurato era anche vittima di cryptomining. Gli aggressori avevano installato nel sistema dell'assicurato un software che stava generando Bitcoin.Il cryptomining si verifica quando il sistema informatico di un soggetto viene utilizzato per il mining di criptovalute a sua insaputa.

**Sezione di copertura applicabile:**

Spese di incident response, Interruzione dell'attività, Recupero di dati e sistemi, Responsabilità derivante da violazioni di obblighi di riservatezza e Responsabilità derivante da violazioni della sicurezza della rete.

**Attenuazione**

Monitorare regolarmente lo stato della sicurezza informatica è importante affinché un'azienda manifatturiera garantisca che la produzione non sia colpita da un attacco. Deve prendere in considerazione piani di disaster recovery e business continuity al fine di minimizzare l'interruzione in caso di attacco. Il controllo degli accessi non è infallibile. Gli aggressori mutano continuamente i loro metodi di attacco e qualsiasi azienda deve rivedere regolarmente la propria sicurezza e le proprie procedure per adeguarsi alla minaccia.

## Il furto di dati si traduce in estorsione, interruzione dell'attività e spese extra

Un'organizzazione sconosciuta ha hackerato la rete di uno studio legale e potrebbe aver ottenuto l'accesso alle informazioni sensibili dei clienti, tra cui l'obiettivo di acquisizione di un'azienda quotata in borsa, una tecnologia potenzialmente brevettabile di un'altra azienda quotata in borsa, la bozza di prospetto di una società di venture capital e un numero significativo di elenchi di class action contenenti Informazioni di Identificazione Personali (PII) dei querelanti.
Un tecnico forense assunto dallo studio legale ha determinato che un malware era stato iniettato all'interno della rete. Subito dopo, lo studio ha ricevuto una chiamata dall'hacker che chiedeva 10 milioni di dollari per non pubblicare online le informazioni rubate. Lo studio legale ha sostenuto 2 milioni di dollari in spese associate alle indagini forensi, alle negoziazioni relative all'estorsione, al pagamento di un riscatto, alla notifica, al monitoraggio del credito e del furto d'identità, ai servizi di ripristino e all'onorario del consulente legale.

**Sezione di copertura applicabile:**

Cyber estorsione, Responsabilità derivante da violazioni di obblighi di riservatezza e Responsabilità derivante da violazioni della sicurezza della rete, Interruzione dell'attività e Spese di incident response.

**Attenuazione**

La formazione del personale al fine di cercare di impedire l'apertura di e-mail sospette è importante. Inoltre si dovrebbe implementare la sicurezza informatica per bloccare i malware qualora si infiltrassero nella rete.

# Medie imprese - Una soluzione Cyber su misura che si adatta alla tua attività

## 1 Servizi di Loss Mitigation per medie imprese

Per aiutare le medie imprese nostre assicurate a mitigare la propria esposizione al rischio cyber, Chubb offre loro numerosi servizi.

**Soluzioni di gestione delle password** incluse nella polizza per un massimo di 500 dipendenti di ciascun assicurato.

- Una gestione efficace delle password può aiutare a minimizzare l'utilizzo non autorizzato di credenziali rubate.

**Simulazioni di eventi di phishing** a scopo formativo sono a disposizione degli assicurati.

- Il phishing è una delle cause di perdite cyber in più rapida crescita, e una semplice formazione per i dipendenti può essere uno strumento efficace per minimizzare un attacco di phishing all'interno delle medie imprese.

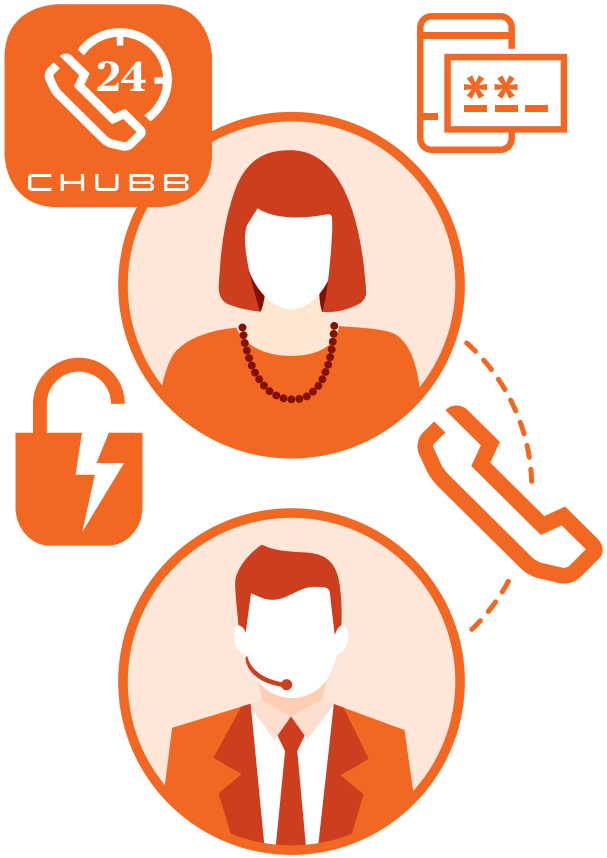
**Clicca qui per maggiori informazioni sul nostro pacchetto completo di servizi cyber, tra cui la sicurezza informatica e altro ancora.**

## 2 Servizi di Incident Response per medie imprese

Rispondere rapidamente e in modo efficace a un evento cyber è fondamentale per minimizzare l'impatto e le perdite: quando accade qualcosa, le nostre polizze cyber mettono a disposizione un panel di esperti fornitori di servizi di Incident Response per le medie imprese nostre clienti. Questi specialisti sono a disposizione 24 ore su 24, 7 giorni su 7, 365 giorni all'anno e sono preparati a guidarti nella ripresa da qualsiasi evento cyber.

- I servizi offerti dagli esperti includono la gestione del processo di incident response, l'informatica forense, le risorse legali, le pubbliche relazioni e negoziatori specializzati in cyber estorsione.
- Flessibilità nell'utilizzo del nostro panel di fornitori o qualsiasi fornitore già incaricato nell'ambito di un piano di cyber incident response.
- Disponibili 24 ore su 24, 7 giorni su 7, 365 giorni all'anno tramite l'app Chubb Cyber Alert®.

**Qui troverai maggiori informazioni su come opera il servizio di Incident Response di Chubb.**



# Medie imprese - Una soluzione Cyber su misura

## 3 Risk Engineering Services

Il modo in cui opera ciascun cliente e la tecnologia che utilizza possono essere differenti in ogni circostanza. I nostri ingegneri specializzati in rischi cyber aiutano i clienti a identificare e comprendere le proprie vulnerabilità tecnologiche e li assistono nel prevenire un evento cyber ancora prima dell'attivazione di una polizza.

### Vantaggi chiave

- **Coinvolgimento diretto dei clienti per acquisire una profonda comprensione del rischio e delle esposizioni**
- **Flessibilità per organizzare incontri con l'assicurato prima della sottoscrizione o in corso di copertura**
- **Raccomandazioni sul rischio e indicazioni su come i clienti possono migliorare il proprio profilo complessivo di gestione del rischio cyber**
- **Formazione tecnica aggiuntiva disponibile per clienti e intermediari**

**Anche se tale servizio è appositamente progettato per i clienti delle medie imprese, può essere preso in considerazione per imprese di qualsiasi dimensione.**

## Il processo

### Come funziona?

**1 Programma pre-indagine**

Obiettivi dell'indagine, punti di discussione, chi dovrebbe essere coinvolto e di quali documenti avremo bisogno prima della riunione.

**2 Indagine - 2-3 ore**

Valutazione di operazioni, sedi, rete e infrastruttura, risorse di sicurezza informatica, processi, politiche e protezioni, specifiche procedure di sicurezza, rilevamento delle violazioni, risposta alle violazioni e incidenti precedenti.

**3 Raccomandazioni**

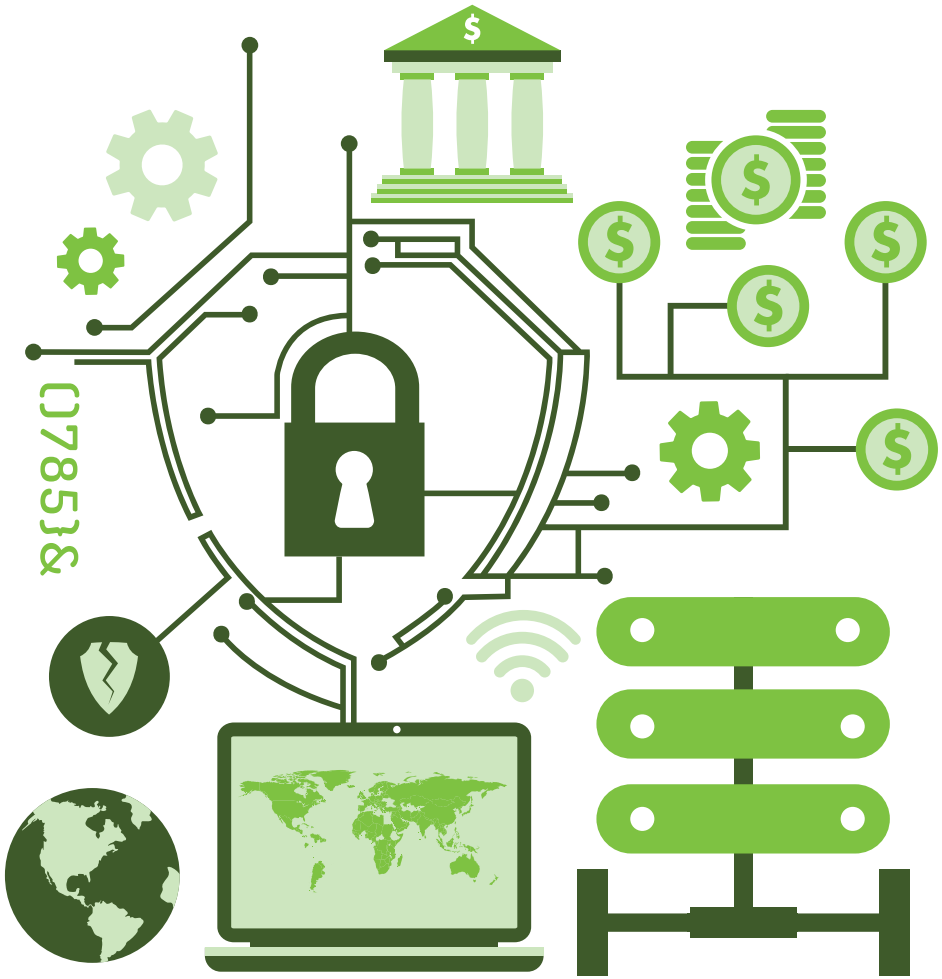
Una volta completata l'indagine, forniremo raccomandazioni specifiche che possono includere potenziali scenari di sinistro e misure mitigatorie da adottare.

**4 Debriefing**

Ci incontreremo con ciascun cliente per spiegare le nostre considerazioni, offrire consigli sui miglioramenti applicabili e collaborare per stabilire le best practice in grado di mitigare un potenziale evento cyber.

# Grandi imprese - Panoramica

Negli ultimi anni, all'aumentare del numero di attacchi informatici a danno di grandi imprese e multinazionali, la domanda di assicurazione cyber è cresciuta rapidamente. La crescente domanda è stata alimentata da una maggiore pressione esercitata sui consigli di amministrazione per dimostrare un'accurata valutazione del rischio cyber, una crescente attenzione alle normative e una più ampia necessità di condivisione delle informazioni tra colleghi e partner. I consigli di amministrazione e i risk manager riconoscono che l'assicurazione cyber dovrebbe andare oltre il semplice trasferimento del rischio. L'offerta di Chubb per le grandi imprese fornisce una soluzione di incident response globale e flessibile, ampie disponibilità di programmi multinazionali, opzioni di captive fronting e capacità significative attraverso la nostra Global Cyber Facility.



**Servizi di Incident Response per grandi imprese**

I piani di cyber incident response vengono spesso stabiliti e frequentemente testati dalle organizzazioni più grandi. I servizi di cyber incident response di Chubb sono volti a integrare ciò che è già in atto. Il nostro team di cyber incident response è pronto a lavorare con i fornitori specializzati scelti dall'assicurato, anche se non fanno parte del panel di Chubb

- La polizza include l'utilizzo di fornitori con cui i nostri clienti hanno concluso contratti come parte di un piano di cyber incident response
- La nostra rete globale di team locali di incident response è progettata per soddisfare le esigenze di rischi multinazionali
- L'app Cyber Alert ® di Chubb, progettata per risk manager o IT manager, si collega al nostro team di gestione sinistri e di incident response per snellire l'assistenza specialistica e la risposta alla polizza

**Qui troverai maggiori informazioni su come opera il servizio di Incident Response di Chubb.**

# Grandi imprese

## 1 Programmi multinazionali

**La natura globale del rischio cyber ha richiesto alle imprese di comprendere il modo in cui le proprie polizze possono rispondere a un evento internazionale** e quali limitazioni potrebbero applicarsi. Strutturare un programma assicurativo multinazionale efficiente e conveniente richiede una comprensione approfondita dell'ambiente regolamentare cyber in evoluzione.

**Alcune domande specifiche quando si prende in considerazione un programma assicurativo multinazionale:**

- Dove sono situate le società controllate? Le limitazioni possono variare da paese a paese.
- I paesi consentono a un assicuratore non autorizzato di pagare le perdite direttamente all'entità locale? Quali sono le limitazioni specifiche del paese?
- Il cliente desidera proteggere gli assicurati localmente? I vantaggi derivanti da una polizza locale includono: pagamento in loco dei sinistri, polizza in lingua locale e gestione locale dei sinistri.

### Capacità su programmi Cyber multinazionali:

**Chubb può offrire programmi Cyber multinazionali a livello locale e coprire oltre 35 Paesi** in tutto il mondo, serviti da tutto il personale del team dei servizi globali di Chubb con competenze e specialisti preparati a fornire assistenza per qualsiasi esigenza assicurativa multinazionale.

## 2 Global Cyber Facility

Una soluzione completa di gestione del rischio cyber per le grandi imprese.

**A chi si rivolge?**

- Organizzazioni con oltre 1 miliardo di dollari di fatturato annuo
- Tutti i settori di attività, tra cui aziende di commercio al dettaglio, istituti finanziari e aziende manifatturiere

**Componenti dell'offerta:**

- Servizi di loss control pre-evento da parte di organizzazioni di sicurezza informatica riconosciute a livello globale al fine di risolvere carenze informatiche identificate durante la valutazione del rischio
- Polizza di trasferimento del rischio
- Incident response post-evento e gestione dei sinistri

**Garanzie chiave della polizza:**

- **Disponibilità di massimali da 30 milioni di dollari a 100 milioni di dollari**
- **Garanzie DIC/DIL disponibili per colmare le lacune** tra polizze cyber, casualty e property di un'organizzazione
- Testo di polizza flessibile

**Qual è il processo?**

- Iniziare in modo proattivo il processo di vendita tre mesi prima dell'ingresso sul mercato
- Valutazione approfondita del profilo di rischio di un'organizzazione
- Collaborazione diretta tra il cliente e gli assuntori di Chubb

# Grandi imprese

## 3 Captives

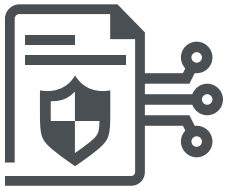
Gestire il rischio cyber all'interno di una captive sta assumendo una rilevanza sempre maggiore per le imprese multinazionali che trovano significativa la combinazione di trasferimento e ritenzione del rischio. Le captives stanno diventando una soluzione comune per mantenere premi adeguati e sostenibili, o per efficientare le franchigie sulla polizza locale all'interno di una struttura consolidata.

Una captive può inoltre fornire una copertura più completa di quella disponibile nel mercato assicurativo della capogruppo. Ciò consente a un'impresa di comprendere le proprie esposizioni e acquisire informazioni sulle perdite in modo che un assicuratore o riassicuratore possa in seguito assumersi il rischio con un limite e un premio appropriati.

| Perché | Come | Sfide |
|---|---|---|
| • Ottimizzare il trasferimento del rischio<br>• Fornire diversificazione<br>• Fungere da incubatore<br>• Accedere a servizi aggiuntivi | • Varie strutture possibili<br>• Piccolo layer primary/ grandi layer di franchigia<br>• Quota contingente di grandi programmi<br>• Rischio specifico | • Incertezza/ comprensione dell'esposizione<br>• Determinazione del prezzo del livello di conservazione<br>• Aggregazione con altre linee |

# Concetti chiave per la vendita

## Non tutti i clienti comprenderanno l'importanza di una polizza assicurativa Cyber o tutti i vantaggi che può offrire. Abbiamo elaborato alcuni concetti chiave per aiutarti a spiegare quali sono i principali vantaggi per i tuoi clienti.



### Protezione esplicita

Le polizze assicurative tradizionali possono essere inadeguate per rispondere alle esposizioni cyber. Una polizza cyber è progettata appositamente per ovviare a tali lacune e fornire un'esplicita protezione contro esposizioni al rischio che potrebbero essere difficili da percepire.

### Non è necessario essere il bersaglio primario di un attacco informatico per subirne le conseguenze.

Gli attacchi informatici possono diffondersi attraverso uno qualsiasi dei tuoi fornitori determinando impatti significativi anche quando non sei il bersaglio primario. Chubb ha avuto prova che da incidenti cyber originatisi presso aziende indipendenti fra loro possono derivare danni collaterali significativi. Cosa succede se il tuo fornitore di servizi di data storage è il bersaglio di un attacco informatico e i tuoi dati vengono compromessi durante il processo?

### L'assicurazione copre le spese di risposta e recupero, non solo la responsabilità derivante dalla compromissione dei dati

La responsabilità derivante dalla perdita o dall'uso improprio di dati sensibili è soltanto una delle potenziali conseguenze di un evento cyber. L'interruzione dell'attività, la fase di incident response e i costi di recupero dei dati costituiscono una parte significativa dei sinistri indennizzati da Chubb, anche in assenza di richieste di risarcimento da parte di terzi.

### Integrazione con i team IT esistenti

L'assicurazione cyber non compromette l'efficacia dei team di sicurezza IT - integra le loro competenze e protegge un'impresa dall'ignoto.

# Concetti chiave per la vendita

### Minacce multinazionali

Le perdite cyber non si verificano solo a livello locale. Chubb aiuta le imprese a riprendersi dagli eventi cyber in tutto il mondo, tra cui violazioni di dati, attacchi ransomware e altri eventi.

### Tutte le imprese possono essere colpite

Gli eventi cyber possono avere un impatto su qualsiasi impresa, indipendentemente da dimensione e settore. Le minacce possono essere mirate, i dipendenti possono commettere errori oppure perdite relative a danni collaterali possono essere causate da un evento cyber più ampio. Chubb offre soluzioni flessibili a seconda delle necessità, del livello di maturità e delle dimensioni dell'impresa.

### Rispondere alla normativa in evoluzione

Le nuove normative sulla privacy prevedono standard e sanzioni sempre più elevati: l'assicurazione cyber può aiutarti a superare tali cambiamenti. Il linguaggio della polizza di Chubb rispecchia le nuove normative sulla privacy in continua evoluzione.

### Adattarsi ai rischi Cyber emergenti

Chubb fornisce le tendenze dei sinistri cyber emergenti su base trimestrale, tenendoti sempre al corrente sui nuovi rischi.Il Chubb Cyber Index® offre inoltre informazioni aggiornate su tendenze recenti e passate.

# Servizi di Loss Mitigation

**La nostra valutazione del trend dei sinistri più comuni ha mostrato temi simili tra i vari settori e i segmenti di clientela. L'errore umano, l'uso improprio e gli attacchi di ingegneria sociale come il phishing sono cause comuni di perdite Cyber ma, con la consapevolezza e la formazione appropriate, possono essere evitati o minimizzati.**

I nostri assicurati hanno accesso a numerosi servizi, tra cui **sicurezza delle password, formazione sul phishing, sensibilizzazione dei dipendenti** e altro ancora.

La nostra filosofia di enterprise risk management dimostra il nostro impegno nel migliorare la gestione del rischio cyber dei nostri clienti. Collaborando con terzi esperti, forniamo ai nostri clienti l'accesso a servizi di miglioramento del rischio cyber facili da applicare, molti dei quali sono gratuiti.

**Per registrarti** ai servizi e avere ulteriori informazioni, visita il sito web Cyber Services di Chubb:

**www.chubb.com/cyber-services**

# Servizi di Loss Mitigation

### 1. Gestione delle password fornito da Dashlane

Le password sono alla base di solide pratiche in materia di sicurezza online. I dati sui sinistri di Chubb mostrano che una gestione inadeguata delle password può portare a perdite cyber significative. Lo strumento di gestione delle password di Dashlane è gratuito per gli assicurati cyber di Chubb.

### 2. Valutazione del livello di consapevolezza in materia di phishing fornito da Cofense

Questo programma di formazione in materia di phishing è progettato per identificare la suscettibilità e il rischio agli attacchi di phishing, un significativo punto debole che ha dato luogo a molte perdite cyber.

### 3. App Chubb Cyber Alert®

Rispondere a un evento cyber può essere molto difficile, e non avere il supporto di specialisti esperti può aumentare le perdite derivanti da un evento. L'app gratuita Chubb Cyber Alert ® fornisce agli assicurati mezzi immediati ed efficienti per segnalare un sinistro e mettersi in contatto con i nostri specialisti di cyber incident response.

### 4. Altri servizi

Per gli assicurati di alcuni paesi sono disponibili corsi di formazione sulla sicurezza informatica, valutazione del rischio, esercizi di pianificazione e altri servizi di Cyber Loss Mitigation. Scopri i servizi disponibili nel tuo paese qui:


**Scopri di più**

www.chubb.com/uk-en/business/cyber-services-registration.aspx

Per ulteriori informazioni, contatta il nostro team di Cyber Risk Advisory cyber@chubb.com

# Servizi di Incident Response - Panoramica

Anche se i servizi di Cyber Loss Mitigation di Chubb possono aiutare a ridurre le probabilità di accadimento di un evento cyber, la realtà è che nessun livello di protezione è perfetto contro le minacce cyber. Le polizze cyber di Chubb includono la nostra rete di specialisti di Incident Response, disponibili 24 ore su 24, 7 giorni su 7, 365 giorni all'anno e preparati per aiutare i nostri assicurati a riprendersi da qualsiasi evento cyber.

## Punti salienti

**Ogni giorno Chubb aiuta le imprese a riprendersi da un sinistro cyber** in tutto il mondo.

Quando gli assicurati comunicano un sinistro cyber attraverso il Centro di Cyber Incident Response di Chubb, riceveranno **assistenza immediata** da parte di uno specialista per raccogliere le informazioni utili a coinvolgere gli esperti adatti a risolvere l'incidente. Il 90% di questi assicurati riceveranno una chiamata da un cyber incident response manager esperto entro 15 minuti.

**Fornitori flessibili** - siamo consapevoli che alcune imprese desiderano utilizzare fornitori che non fanno parte della nostra rete. Chubb offre agli assicurati la flessibilità di utilizzare specialisti di loro scelta in molti paesi che possono essere facilmente inclusi all'interno della nostra rete di incident response.

Scopri come funziona il nostro processo di incident response qui:

**Avanti**

# Servizi di Incident Response - Come funzionano

Questa guida spiega come accedere al team di Cyber Incident Response di Chubb, come segnalare un sinistro e cosa aspettarsi dalla nostra piattaforma di Incident Response.

## 1 Il cliente subisce un evento Cyber

La piattaforma di Incident Response di Chubb è disponibile 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Fornisce accesso al Centro di Cyber Incident Response di Chubb e al nostro team di Cyber Incident Response e offre un approccio olistico alla gestione degli eventi cyber.

## 2 Il cliente segnala l'evento Cyber utilizzando uno qualsiasi dei seguenti metodi:

**Applicazione per smartphone Chubb Cyber Alert®**

Disponibile nell'Apple Store e in Google Play Store

Download on the App Store | ANDROID APP ON Google play

**Online**

Accesso alla nostra piattaforma: **www.chubbcyberalert.com**


**Numero verde**

Individua il tuo numero verde locale di seguito:

### Numeri verdi locali

| | |
|---|---|
| Argentina | **800 666 1967** |
| Australia | **1 800 027428** |
| Austria | **0800 005 376** |
| Belgio | **800 49 405** |
| Brasile | **0800 095 7346** |
| Canada | **1 866 561 8612** |
| Cile | **1 230 020 1212** |
| Cina | **400 120 5310** |
| Colombia | **01 800 518 2642** |
| Repubblica Ceca | **800 142 853** |
| Danimarca | **80 250 571** |
| Finlandia | **0 800 1 12382** |
| Francia | **08 05 10 12 80** |
| Germania | **0800 589 3743** |
| Hong Kong | **800 900 659** |
| Indonesia | **001 803 011 2974** |
| Irlanda | **1 80 093 7331** |
| Israele | **1 80 921 3812** |
| Italia | **80 019 4721** |
| Giappone | **00531 1 21575** |
| Corea del Sud | **00798 14 800 6017** |
| Malesia | **1 800 8 12541** |
| Messico | **001 855 250 4580** |
| Paesi Bassi | **0800 020 3267** |
| Nuova Zelanda | **0800 441402** |
| Norvegia | **800 12554** |
| Panama | **001 800 507 3360** |
| Perù | **0800 56006** |
| Polonia | **00 800 121 4960** |
| Portogallo | **800 8 14130** |
| Singapore | **800 120 6727** |
| Sudafrica | **080 09 82340** |
| Spagna | **800 810 089** |
| Svezia | **020 088 3181** |
| Svizzera | **080 016 6223** |
| Taiwan | **00801 13 6828** |
| Turchia | **0811 213 0171 (landline)** |
| Turchia | **0812 213 0043 (mobile)** |
| EAU | **8000 444 4411** |
| Regno Unito | **0800 279 7004** |
| Stati Uniti | **1 844 740 9227** |
| Vietnam | **1203 2353 (VNPT)** |
| Vietnam | **1228 0688 (Viettel)** |

# Servizi di Incident Response - Come funzionano

## 3 Contatto dal Centro di Incident Response di Chubb


**Entro 1 minuto** dalla segnalazione di un evento, il cliente sarà messo in contatto con un consulente per raccogliere le seguenti informazioni:

- Nominativo dell'assicurato
- Paese in cui è stata emessa la polizza
- Recapiti
- Posizione dell'evento

Le informazioni saranno inviate al team locale di Incident Response Management e possono essere inviate all'Ufficio Sinistri di Chubb. Mantenere informata Chubb garantirà una gestione del sinistro più efficiente.

## 4 Incident Response Management


**Entro 1 ora** dalla segnalazione, il cliente riceverà una telefonata dall'Incident Response Manager locale dove si è verificato l'evento. Le fasi successive includono:

- Condurre un'indagine iniziale
- Sviluppare un piano d'azione per contenere l'evento
- Nominare specialisti per fornire consigli e supporto nella ripresa:

Informatica forense | Consulenza legale | Pubbliche relazioni | Conformità normativa | Protezione dell'identità | Monitoraggio del credito | Contabilità forense

## 5 Ripristino

Con un panel di fornitori esperti che lavorano al fine di contenere l'evento, il team di Cyber Incident Response ti supporterà nel ripristino delle attività aziendali.

## 6 Follow-up

I fornitori specializzati di Chubb valuteranno la possibilità di fornire servizi aggiuntivi per assisterti nell'analisi dell'evento, al fine di includere azioni correttive future, una revisione delle lezioni apprese e consigli sulla mitigazione del rischio.

# Garanzie di polizza - Cyber Enterprise Risk Management

## Le garanzie

### Copertura per danni propri

- **Incident Response** - da un evento cyber effettivo o sospetto
- **Interruzione dell'attività** - perdita del margine operativo
- **Recupero di dati e sistemi** - aumento del costo del lavoro, costi di recupero dei dati, costi aggiuntivi per la mitigazione dell'interruzione dell'attività
- **Estorsione di rete** - pagamenti e negoziazione dell'estorsione

### Copertura per danni a terzi

- **Responsabilità derivante da eventi cyber, violazioni di obblighi di riservatezza e violazioni della sicurezza della rete** - responsabilità risultante da una violazione dei dati o da falle nella sicurezza della rete:
  - **Penalità derivanti da carte di pagamento:** responsabilità contrattuali dovute alle imprese del settore delle carte di pagamento a seguito di un incidente cyber
  - **Fondo di risarcimento per i consumatori**
  - **Multe e sanzioni normative** (dove legalmente assicurabili)
- **Responsabilità derivante dai media** - responsabilità a seguito di diffamazione o violazione della proprietà intellettuale online

## I punti salienti

- **Interruzione contingente dell'attività** a causa dei fornitori esterni di servizi IT
- **Errori di sistema** errore umano, errore di programmazione, interruzione di corrente
- **Estensioni standard:**
  - **Spese di emergenza di Incident Response** entro 48 ore per le PMI e le aziende di medie dimensioni
  - **Costi di miglioramento** - miglioramento del software e delle applicazioni
  - **Cyber crime** - perdita finanziaria diretta a seguito di furto cyber
  - **Spese di ricompensa**
  - **Frode nelle telecomunicazioni**
- **Pagamento per conto dell'assicurato** delle spese di incident response
- **Fornitori di incident response flessibili**
- **Dipendente infedele**
- **Notifica volontaria**
- **Interruzione volontaria**
- **Danni reputazionali***
- **Frode di ingegneria sociale***
- La prima copertura del settore contro gli eventi cyber a impatto diffuso

* con apposita estensione

# Estensioni

## Chubb affronta i crescenti rischi Cyber con un approccio flessibile e sostenibile. Gli assicurati possono personalizzare i livelli della copertura assicurativa Cyber per Eventi a Impatto Diffuso, Ransomware e Perdite per Sfruttamento Software Trascurato.

### 1 Eventi a Impatto Diffuso

Il mondo sta diventando ogni anno più digitalizzato e interconnesso. Migliaia se non milioni di aziende si affidano a programmi software, piattaforme di comunicazione e tecnologie ampiamente diffusi. Un singolo attacco o un guasto a una di queste piattaforme o tecnologie ampiamente utilizzate potrebbe creare un rischio aggregato in grado di mettere alla prova la capacità di risposta del settore assicurativo. Al fine di fornire agli assicurati maggiore certezza di copertura e stabilità del mercato assicurativo, Chubb offre limiti, franchigie e coassicurazione personalizzabili e specifici per tali "Eventi a Impatto Diffuso".

**Le tipologie di Eventi a Impatto Diffuso coperte includono**

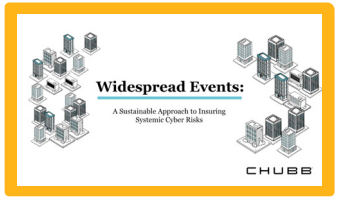
- **Sfruttamento di vulnerabilità nella supply chain del software**
  Si tratta di attacchi che consentono ai malintenzionati di accedere ai sistemi attraverso un software affidabile e certificato e rappresentano di fatto un cavallo di Troia per i sistemi
- **Sfruttamento di vulnerabilità zero-day**
  Si tratta di attacchi derivanti dallo sfruttamento di determinate vulnerabilità del software note ai criminali informatici ma non ancora a nessun altro. Queste vulnerabilità che possono essere facilmente sfruttabili, sono gravi e spesso prive di protezione
- **Sfruttamento di vulnerabilità note**
  Si tratta di attacchi derivanti dallo sfruttamento di vulnerabilità note del software alle quali non sono state applicate patch di sicurezza. Le vulnerabilità sono classificate come "Severe" poiché sono facili da sfruttare, possono essere diffuse da remoto con privilegi di accesso limitati e possono causare danni significativi
- **Tutti gli altri Eventi a Impatto Diffuso**
  Alcuni tipi di attacchi cyber possono essere condotti simultaneamente o automaticamente contro un ampio numero di vittime, provocando in ultima istanza un evento cyber dalle proporzioni catastrofiche. Internet e alcuni servizi di telecomunicazione rappresentano oggi un'infrastruttura sociale critica. Alcune grandi aziende di cloud computing sono così ampiamente utilizzate che un'interruzione potrebbe avere un impatto sulle operazioni commerciali di migliaia o addirittura milioni di aziende.

**Casi reali di Eventi a Impatto Diffuso:**

- Sfruttamento di vulnerabilità nella supply chain del software: Solorigate (2020), NotPetya (2017)
- Sfruttamento di vulnerabilità zero-day: Hafnium (2021)
- Sfruttamento di vulnerabilità note: MSSP Attack (2021)
- Altri Eventi a Impatto Diffuso: Virginia Cloud Outage (2020)

**L'appendice per Eventi a Impatto Diffuso prevede disposizioni pratiche e sintetiche nel merito dell'operatività della copertura, tra cui:**

- Le spese di incident response non sono soggette ai sottolimiti di copertura per Eventi a Impatto Diffuso fino a quando non viene stabilito che si tratta di un Evento a Impatto Diffuso e non è prevista la restituzione all'assicuratore delle spese sostenute prima di tale determinazione
- Gli assicurati possono decidere di non condividere le informazioni emerse dalle indagini quando viene appurato che un incidente è un Evento a Impatto Diffuso
- Per consentire agli assicurati di acquistare la copertura che meglio soddisfa le esigenze della propria attività, tutti gli incidenti cyber sono classificati come Eventi a Impatto Limitato (ad esempio un evento locale che sarà gestito attraverso le politiche standard di gestione del sinistro) o Eventi a Impatto Diffuso (ad esempio un evento sistemico che sarà gestito considerando limiti, franchigie e scoperti dedicati).




**Eventi a Impatto Diffuso**

[1]NIST Security Vulnerability Trends in 2020: An Analysis (2021). Consultabile all'indirizzo https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.

# Altre sezioni di copertura

## 2 Ransomware

Gli attacchi ransomware sono aumentati notevolmente sia in termini di frequenza sia di gravità. Le perdite per gli assicurati sono molto più ampie del semplice valore dell'importo del riscatto. Indipendentemente dal fatto che il riscatto sia pagato o meno, gli assicurati spesso sostengono spese legali, spese di indagine forense, perdite per interruzione dell'attività, costi di ripristino dei dati digitali e, potenzialmente, costi di responsabilità civile e di difesa legale.

L'estensione per ransomware consente di personalizzare i limiti di copertura, le franchigie e la coassicurazione per i danni subiti a seguito di un attacco ransomware.

## 3 Vulnerabilità di Software Trascurato

Mantenere aggiornati i software è un aspetto importante in materia di cyber hygiene. Molti danni possono essere prevenuti applicando patch al software vulnerabile prima che i criminali informatici abbiano l'opportunità di sfruttarlo, tuttavia alcune aziende potrebbero non intervenire immediatamente. A volte ci sono ragioni legittime per cui gli aggiornamenti software devono essere testati prima di essere implementati e la compatibilità, la capacità o semplici problemi logistici possono impedire, anche a un'azienda ove la sicurezza informatica è ben gestita, di applicare le patch entro il primo giorno o la prima settimana dal rilascio. Per questo motivo, Chubb offre agli assicurati un periodo di 45 giorni per correggere le vulnerabilità del software pubblicate come Common Vulnerabilities and Exposures (CVE) all'interno del National Vulnerability Database gestito dal National Institute for Standards and Technology (NIST) degli Stati Uniti.

L'estensione per Vulnerabilità di Software Trascurato fornisce copertura dopo la scadenza del periodo di 45 giorni, con una condivisione del rischio tra l'assicurato e l'assicuratore che si sposta gradualmente sull'assicurato, il quale si assume progressivamente una parte maggiore del rischio se la vulnerabilità non viene corretta al 46°, 90°, 180° e 365° giorno.


**Sfruttamento di Software Trascurato**

# Appetiti assuntivi

**Per consentirti di supportare in modo ottimale i tuoi clienti, abbiamo creato il seguente riepilogo dei nostri appetiti. Non è un elenco esaustivo, ma fornisce alcune indicazioni generali. Per rischi o settori particolari non elencati di seguito, contatta il nostro team di sottoscrizione per discutere delle tue esigenze.**

## Preferiti

- Pubblicità*
- Agricoltura
- Architetti e ingegneri
- Gallerie d'arte e musei
- Concessionari automobilistici e stazioni di servizio
- Prodotti chimici e affini
- Comunicazioni*
- Edilizia
- Produzione/fabbricazione alimentare
- Appaltatori generali
- Consulenti aziendali
- Consulenti di marketing
- No-profit
- Arti dello spettacolo e teatri*
- Stampa e pubblicazione*
- Produzione manifatturiera
- Settore immobiliare
- Consulenti tecnici
- Associazioni commerciali
- Produzione televisiva/ radiofonica/cinematografica*
- Commercio all'ingrosso

## Accettati

- Contabili
- Operatori delle professioni sanitarie
- Gestori patrimoniali
- Hardware/software per computer
- Enti depositari
- Studi medici/odontoiatrici
- Agenzie di collocamento/ Agenzie di selezione del personale
- Servizi di ingegneria e gestione
- Istituti finanziari - Non altrimenti elencati
- Produzione industriale
- Gestori di investimenti/fondi
- Studi legali
- Intermediari ipotecari
- Servizi personali
- Servizi professionali - Non altrimenti elencati
- Ristoranti/Settore alberghiero
- Commercio al dettaglio
- Servizi di trasporto - Non altrimenti elencati

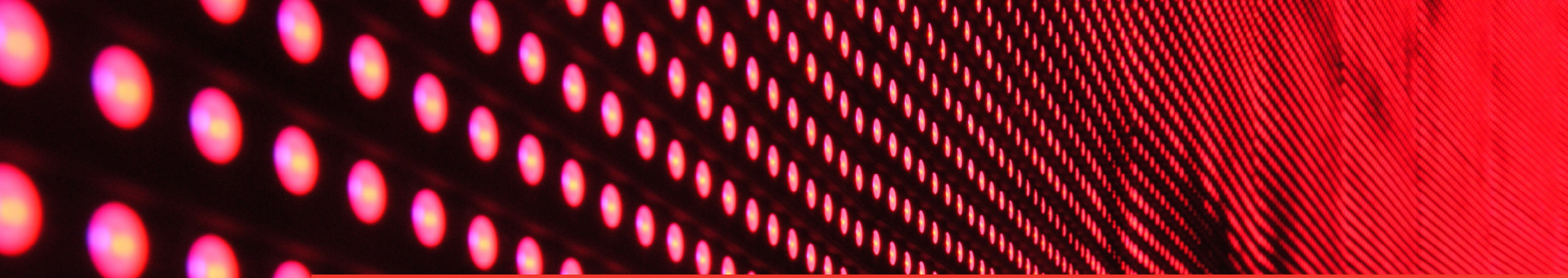
## Selettivi

- Residenze Sanitarie Assistenziali
- Servizi di fatturazione
- Emittenti Radio e TV*
- Call Center
- Agenzie di recupero crediti
- College e università
- Commercianti di materie prime
- Cambiavalute
- Enti governativi
- Ospedali
- Assicurazione - Linee non personali
- Notai
- Case di cura/riposo
- Pubblica amministrazione
- Autorità pubbliche
- Banche commerciali
- Intermediari in titoli e merci
- Scuole di piccole dimensioni/ Consiglio di amministrazione scolastico dal nido alla scuola media
- Telecomunicazioni
- Servizi di telemarketing*
- Agenti di titolo
- Utilities/Servizi pubblici

## Vietati

- Contenuti per adulti
- Compagnie aeree
- Scambi di criptovalute
- ICO (Initial Coin Offering)
- Aggregatori di dati
- Borse online
- Siti/Applicazioni di social network
- Piattaforme commerciali

*Escluse le coperture di RC Professionale dei Media



CHUBB®

# Per maggiori informazioni

Per saperne di più sulla nostra offerta Cyber, contatta i nostri assuntori oppure visita il sito **www.chubb.com/it/cyber**



Torna all’inizio

IT7555-MD 10/22