Chubb Cyber Enterprise Risk Management – Versione 2.2

Principali caratteristiche

CHUBB®

Chi protegge la polizza?

Cyber Enterprise Risk Management protegge le organizzazioni di qualunque dimensione da disastri quali indisponibilità, perdita, violazione e corruzione dei dati, ransomware ed eventi derivanti dai contenuti multimediali online, sia per danni a terzi, sia per danni propri causati da atti malevoli e/o negligenza.

La polizza comprende una vasta gamma di soluzioni per la valutazione del rischio Cyber, la gestione della crisi successiva all'evento e il trasferimento del rischio che oggi le aziende sono chiamate a fronteggiare.

Perché le aziende hanno bisogno di questa copertura assicurativa?

Costi crescenti

Le violazioni degli obblighi di riservatezza possono costare alle aziende fino a 3,6 milioni di dollari per evento, a seconda della gravità dell'attacco.

Minacce crescenti

Anche le aziende con solide misure di sicurezza informatica e solide politiche in materia di privacy sono esposte al crimine informatico.

I dati sui sinistri di Chubb gestiti negli ultimi 20 anni mostrano che il numero dei dati personali dei nostri assicurati ammonta a oltre 500 milioni di record.

Il ransomware, uno degli attacchi più comuni, ha registrato un aumento significativo in termini di frequenza e gravità delle perdite dal 2019.

Cosa include la polizza?

Incident Response: gli assicurati di Chubb hanno accesso alla nostra rete di società specializzate in servizi di Incident Response Management in tutto il mondo, tramite un numero verde dedicato, l'applicazione per mobile Chubb Cyber Alert o il sito Chubb Cyber Alert. Supportiamo i clienti durante un incidente utilizzando una rete di esperti in ambito forense, di risposta agli attacchi denial of service, Cyber-estorsione, consulenza legale, attività di notifica, risposta alle frodi e pubbliche relazioni. Questo servizio è disponibile 24 ore al giorno, 365 giorni all'anno.

La copertura per responsabilità civile: protegge l'assicurato dai danni causati dalla violazione di dati personali e informazioni aziendali confidenziali. Le principali coperture previste sono:

- Violazione degli obblighi di riservatezza: mancata protezione dei record e dei dati in formato cartaceo e/o digitale
- Sicurezza della rete: trasmissione di un attacco informatico a terzi
- Contenuti multimediali: violazione della proprietà intellettuale a causa di errata gestione dei dati o di negligenza nell'uso dei contenuti pubblicati online
- Accesso negato: limitazione della possibilità per i clienti di accedere ai sistemi informatici dell'assicurato, ad esempio siti web, a causa di un attacco al sistema
- Reputazione: diffamazione o violazione della privacy tramite un'attività informatica

La copertura per i danni propri: ha l'obiettivo di minimizzare gli effetti di un incidente Cyber. Le principali coperture previste sono:

- Spese di notifica per violazione di dati personali
- Riduzione del margine di profitto a causa dell'interruzione dell'attività
- Costi di recupero e ripristino dei dati, compreso l'aumento del costo del lavoro e delle apparecchiature
- Danni e spese per Cyber-estorsione
- Spese per la gestione della crisi a seguito di un incidente: la polizza risponde con una serie di fornitori specializzati nella gestione adeguata e tempestiva dell'incidente

Le estensioni includono le spese di emergenza di incident response, i costi di miglioramento, il crimine informatico, le spese di ricompensa e le frodi relative alle telecomunicazioni.

Offriamo la copertura contro le azioni delle autorità di vigilanza per le violazioni degli obblighi di riservatezza dei dati, ove assicurabili per legge. Essa include i costi di difesa, le sanzioni comminate dall'autorità e i pagamenti per l'indennizzo dei consumatori.

Il nostro team europeo di ingegneri fornisce ai clienti servizi di Risk Engineering e di mitigazione del danno.

Qual è il massimale?

Fino a € 3 milioni per alcuni settori su base annuale.

Principali vantaggi della copertura

Copertura/Servizi	Vantaggi
Spese di emergenza di incident response	Spese di IT forensic sostenute nelle prime 48 ore al fine di investigare un potenziale incidente Cyber.
Crimine Informatico	Sottolimite per perdite di denaro o titoli dovuti ad atti informatici dolosi commessi da soggetti esterni.
Costi di miglioramento	Sottolimite per i costi di miglioramento per potenziare o migliorare i software del tuo sistema informatico a seguito di un incidente.
Approccio alla copertura modulare e flessibile	I clienti possono scegliere le garanzie in base alle proprie esigenze, tra cui la pienezza del massimale per le spese di notifica per violazione degli obblighi di riservatezza e i costi di gestione della crisi, ove pertinente.
Notifica Volontaria	La garanzia avente ad oggetto la copertura dei costi di notifica per violazione della riservatezza può essere attivata anche nei casi in cui non vi è obbligo di notifica alle autorità o alle persone interessate.
Copertura delle informazioni aziendali	La copertura non è limitata alla violazione dei dati personali, ma comprende anche le informazioni aziendali riservate.
Azioni, sanzioni e multe dell'autorità di vigilanza	La polizza di Chubb offre una copertura completa delle sanzioni delle autorità di vigilanza (dove la legge lo consente), dei costi di difesa dalle azioni dell'autorità e dei pagamenti per l'indennizzo del consumatore.
Minacce interne ed esterne	La polizza non si limita alle minacce esterne; possono essere coperte anche le violazioni della sicurezza interne causate da dipendenti 'infedeli'.
Costi di monitoraggio del credito	Le spese di notifica per violazioni della riservatezza di Chubb prevedono servizi di monitoraggio del credito per tutelare le persone dall'uso fraudolento dei propri dati personali.
Copertura in tutto il mondo	La polizza opera con territorialità estesa al mondo intero per rispondere alla natura multinazionale del rischio Cyber.
Cyber Estorsione	Forniamo copertura per i danni e i costi associati alla mitigazione di un incidente di Cyber-estorsione, compreso il pagamento del riscatto, ove consentito dalla legge.
Servizio di Incident Response	Il nostro servizio di risposta agli incidenti prevede una hotline in lingua locale attiva 24/7, 365 giorni all'anno, supportata da un piano di risposta agli incidenti chiavi in mano con esperti globali e locali, mantenendo il diritto del cliente di scegliere i fornitori più adatti a gestire l'incidente. I clienti possono segnalare un sinistro tramite la nostra app Cyber Alert, il sito Web o con una semplice telefonata.

Principali vantaggi della copertura

Copertura/Servizi	Vantaggi
Perdite per interruzione dell'attività aziendale	Include la perdita di profitto e le spese extra derivanti da un incidente Cyber.
Costi di recupero dei dati e dei sistemi	Comprende i costi di recupero di dati e sistemi a seguito di un incidente Cyber, nonché altri costi per mitigare le perdite dovute all'interruzione dell'attività.
Errore di sistema	Per errori dell'amministratore IT, o a causa di un errore umano, o per errori di programmazione che portano a un evento di interruzione dell'attività o perdita dei dati.
Outsourcing dei sistemi in caso di crisi	La nostra copertura comprende anche il costo dell'outsourcing dei sistemi in caso di crisi a seguito di un attacco *denial of service*.
Penali contrattuali	Copriamo le penali contrattuali o gli accertamenti derivanti da PCI DSS (Payment Card Industry Data Security Standard), nonché il costo d'ingaggio di un Investigatore Forense PCI approvato per determinare le perdite.
Media liability	Forniamo copertura per responsabilità derivante dai contenuti multimediali pubblicati online dall'assicurato, compresi i siti di social media sotto il suo controllo.
Contingent Business Interruption	Include molti scenari in cui un incidente Cyber ha un impatto su un fornitore di servizi IT in outsourcing (ad es. backup, cloud, hosting)

Cosa cambia nel wording di polizza Enterprise Risk Management Versione 2.2?

1. **Sistema informatico assicurato e sistema informatico condiviso**
   C'è ora una netta divisione tra gli incidenti Cyber che impattano l'infrastruttura di rete controllata dagli assicurati e quelli che hanno invece un impatto sulle infrastrutture gestite dai loro fornitori di servizi IT.

2. **Ransomware**
   Le perdite per gli assicurati sono nettamente più ingenti rispetto al mero ammontare del riscatto. L'estensione ransomware consente di personalizzare i limiti di copertura, le franchigie e lo scoperto per i danni subiti a seguito di attacchi ransomware.

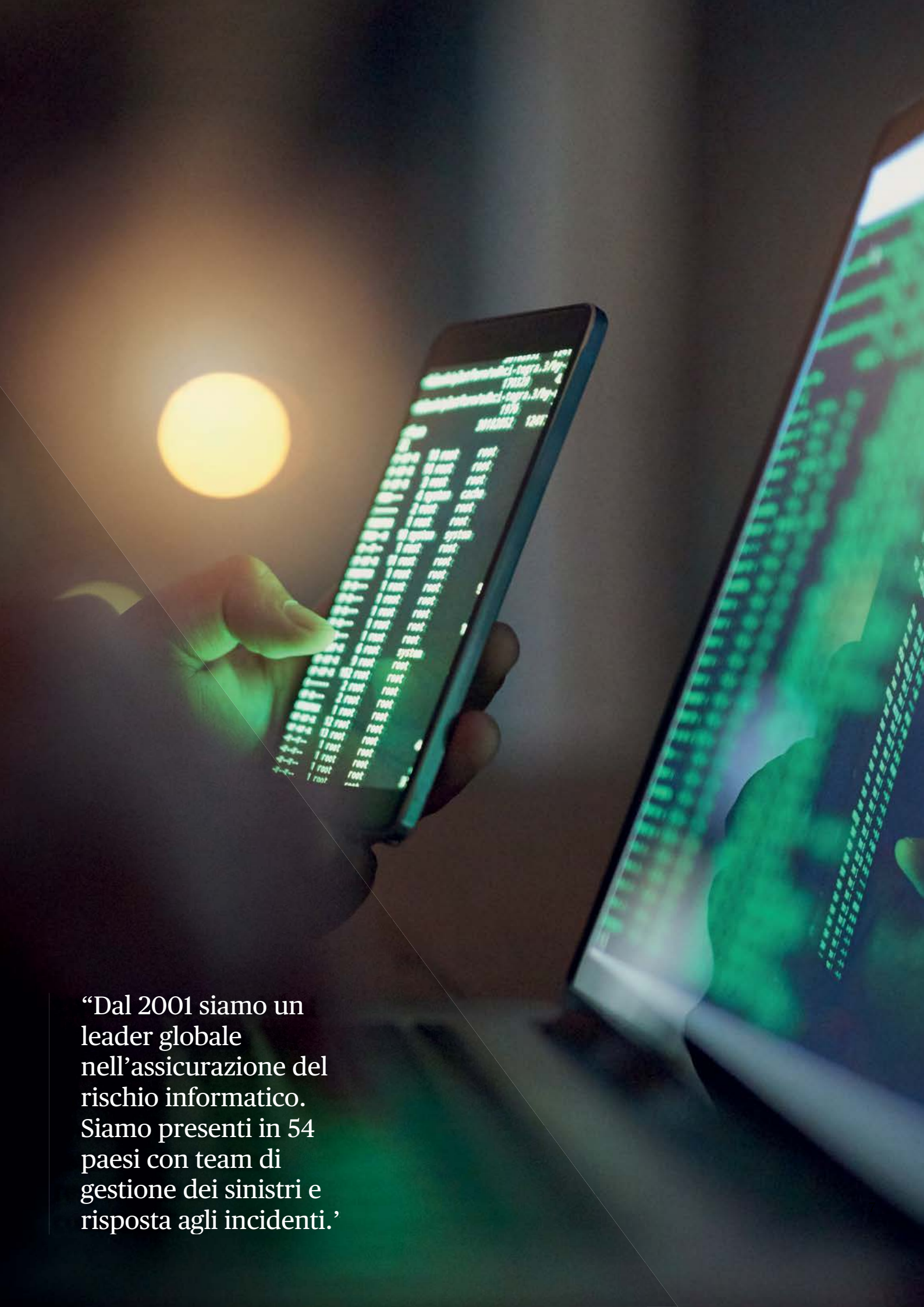
3. **Vulnerabilità di Software Trascurato**
   A volte ci sono ragioni legittime per cui gli aggiornamenti software devono essere testati prima di essere implementati e la compatibilità, la capacità o semplici problemi logistici possono impedire anche a un'azienda di sicurezza informatica ben gestita di applicare le patch immediatamente. Per questo motivo, Chubb offre agli assicurati un periodo di 45 giorni per applicare le patch relative alle 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'appendice 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.

4. **Eventi a Impatto Diffuso**
   La garanzia 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
   - Gli assicurati possono decidere di non condividere le informazioni emerse dalle indagini quando viene appurato di comune accordo che un incidente è un Evento a Impatto Diffuso
   - Gli assicurati possono acquistare la copertura che meglio soddisfa le loro esigenze, scegliendo tra varie opzioni di copertura per eventi a impatto limitato o eventi a impatto diffuso

Guarda il nostro video per saperne di più >

5. **Esclusioni aggiornate:** infrastrutture, azioni di autorità pubbliche, guerra, violazioni di leggi degli Stati Uniti d'America, RC professionale. Le esclusioni base sono state aggiornate in linea con le tendenze e l'analisi del rischio sistemico.



“Dal 2001 siamo un leader globale nell’assicurazione del rischio informatico. Siamo presenti in 54 paesi con team di gestione dei sinistri e risposta agli incidenti.’

I nostri target assicurativi

Settori preferiti:

- Servizi professionali e consulenza
- Manifatturiero ed edilizia
- Media
- Intrattenimento e alberghiero
- Vendita al dettaglio
- Grande Distribuzione
- Real estate

Settori non accettati:

- Payment processing/circuiti carte di credito
- Aggregatori di dati e/o gestori di banche dati
- Gioco online
- Social network
- Infrastrutture critiche
- Piattaforme di trading

Perché scegliere Chubb?

Competenze specializzate nel rischio informatico. Dal 2001 siamo uno dei leader globali nell'assicurazione dei rischi informatici.

Diffusione globale. Le nostre polizze offrono una copertura globale per rispondere alla costante evoluzione del panorama normativo. In 54 Paesi abbiamo team locali di gestione dei sinistri e di risposta agli incidenti, compresi team di assuntori dedicati nei principali Paesi, al fine di mantenere elevato il livello di servizio in tutto il mondo.

Enterprise Risk Management. Il nostro approccio olistico ci consente di fornire copertura per i danni propri e i danni a terzi oltre ad offrire servizi di valutazione preventiva del rischio, servizi di gestione delle crisi post-evento e soluzioni di trasferimento del rischio.

Ulteriori coperture
Offriamo una vasta gamma di prodotti finanziari fra cui:

- Crime - Atti di infedeltà dei dipendenti
- D&O - Responsabilità civile degli amministratori

Il presente documento è destinato unicamente a broker assicurativi professionisti ed a scopo meramente informativo. Per il dettaglio di termini, condizioni ed esclusioni della polizza consultare il fascicolo informativo.

Contatti

Chubb
Rappresentanza Generale per l'Italia
Via Fabio Filzi, 29 - 20124 Milano
T: 02 27095.1
E: info.italy@chubb.com

chubb.com/it

Chubb. Insured.℠

IT8194-MD 05/22