



Chi protegge la polizza

Cyber Enterprise Risk Management protegge le organizzazioni di qualunque dimensione da disastri quali perdita, indisponibilità e corruzione dei dati, violazione degli obblighi di riservatezza, ransomware ed eventi derivanti dai media online, sia in termini di responsabilità civile, sia per le perdite causate da atti dolosi 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 i clienti hanno bisogno di questa copertura?

Costi crescenti

- Le violazioni degli obblighi di riservatezza possono costare alle aziende fino a 4 milioni di dollari* per evento a seconda della gravità dell'attacco
- Nel 2015 il costo medio per record perso o rubato ha raggiunto i 158 dollari*
- Rispetto al 2013 il costo totale di una violazione dei dati è cresciuto del 29%**

Minacce crescenti

Le versioni di ransomware sono cresciute da poco meno di 400.000 nella seconda metà del 2014 ad oltre 2 milioni nella prima metà del 2015***. Il ransomware sta diventando una delle più pericolose minacce cyber che le organizzazioni devono affrontare, con perdite globali per milioni di euro.

Anche le società con una solida sicurezza informatica e ottimi controlli della riservatezza dei dati sono esposte al crimine informatico.

*(IBM & Ponemon Institute 2016 Cost of Data Breach Study)

** (McAfee Labs 2016 threat predictions report)

*** (Symantec Special Report 2016 Ransomware and Businesses)



Cosa include?

La risposta agli incidenti: abbiamo creato una partnership con un leader globale nella gestione delle crisi per offrire ai clienti una risposta agli incidenti 24/7 su scala globale, attraverso un numero verde indicato in polizza. Il nostro partner assiste i clienti in tutte le fasi del processo, impiegando una rete di esperti in ambito informatico: risposta agli attacchi *denial of service*, cyber-estorsione, consulenza legale, attività di notifica, risposta alle frodi e pubbliche relazioni. Questo servizio è disponibile in lingua locale 24 ore al giorno, 365 giorni all'anno.

La copertura per la responsabilità civile: protegge l'assicurato dai danni causati dalla violazione di dati personali e informazioni aziendali protette da accordi di riservatezza. 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
- Contenuti multimediali: violazione di una proprietà intellettuale a causa di errata gestione dei dati o di negligenza nell'uso dei media
- 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 perdite dirette: ha l'obiettivo di minimizzare gli effetti di un incidente informatico. Le principali coperture previste sono:

- Spese di notifica
- 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.

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

Il nostro team di tecnici in tutto il mondo fornisce ai clienti servizi di Risk Engineering e di mitigazione del danno.

A quanto ammonta il massimale?

Fino a 20 milioni di euro su base aggregata.

Principali vantaggi della copertura

Copertura / Servizi	Vantaggi
Approccio alla copertura modulare e flessibile	I clienti possono scegliere le coperture in base alle proprie esigenze. Le garanzie sono prestate nella pienezza del limite di risarcimento, anche per quanto riguarda la violazione degli obblighi di riservatezza, costi di notifica e spese di gestione.
Notifica volontaria	La garanzia avente ad oggetto la copertura dei costi di notifica può essere attivata anche nei casi in cui non vi è obbligo di notifica in capo all'assicurato.
Nessuna necessità di aggiornamenti, adeguamenti e controllo	La nostra polizza non prevede esclusioni della copertura in caso di mancato aggiornamento, adeguamento o mantenimento della policy di sicurezza dei sistemi da parte del cliente.
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 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.
Ampiezza della copertura	Copriamo anche il 'presunto' accesso non autorizzato ai sistemi informatici, per cui l'assicurato non ha l'onere della prova. Questo significa che offriamo copertura per una più vasta gamma di eventi o situazioni.
Minacce interne ed esterne	La polizza non si limita alle minacce esterne; possono essere coperte anche le violazioni della sicurezza causate da dipendenti 'infedeli'.
Costi di monitoraggio del credito	Le spese di notifica per violazioni della riservatezza prevedono servizi di monitoraggio per tutelare le persone verso l'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 informatico.
Copertura dei fornitori esterni di servizi	La copertura si estende ai sistemi informatici gestiti per conto dell'assicurato da fornitori esterni e partner aziendali, ad esempio, backup, cloud o hosting.
Estorsione informatica	Forniamo copertura per i danni e i costi associati alla mitigazione di un incidente di cyber-estorsione, compreso il pagamento di riscatti ove consentito dalla legge.
Risposta agli incidenti	Il nostro servizio di risposta agli incidenti prevede una hotline in lingua locale attiva 24/7, supportata da un piano di risposta agli incidenti con esperti globali e locali, mantenendo il diritto del cliente di scegliere i fornitori più adatti a gestire l'incidente.
Interruzioni dell'attività e spese extra	Comprende l'aumento dei costi del lavoro e di noleggio di apparecchiature derivanti da una perdita di disponibilità dei sistemi e/o dei dati, comprese interruzioni di corrente, sbalzi di tensione, o limitazione o interruzione del servizio.

Copertura / Servizi	Vantaggi
Costi di recupero dei dati	Comprende i costi di recupero derivanti da perdite di dati per interruzioni della fornitura di energia, sbalzi di tensione o limitazione del servizio indipendentemente dal fatto che il sistema di alimentazione sia controllato dall'assicurato.
Errore in buona fede	Per errori dell'amministratore IT, o per errore umano, o per errori di programmazione che portano a un evento di interruzione dell'attività o di 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 <i>denial of service</i> .
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.
Responsabilità media	Forniamo copertura per responsabilità derivante dai contenuti multimediali pubblicati online dall'assicurato, compresi i siti di social media.

