Ania

Associazione Nazionale
fra le Imprese Assicuratrici

IL RISCHIO CYBER

CONOSCERLO DI PIÙ PER PROTEGGERSI MEGLIO

IL RISCHIO CYBER E I TIPI DI INCIDENTE

Il rischio cyber è al 2° posto tra i rischi più temuti dalle aziende

La tecnologia sta costantemente trasformando le nostre vite e migliorando l'operatività di tutte le realtà produttive determinando però nuove vulnerabilità che, se non previste, possono causare danni irreparabili.

Il 12 maggio 2017 è la data dell'attacco informatico più spaventoso mai avvenuto: WannaCry, che si diffuse in poche ore, in 150 Paesi, infettando più di 200.000 macchine e provocando un danno di oltre 4 miliardi di dollari. Un anno dopo, il 97% delle aziende è ancora vulnerabile esattamente come prima.

Le continue notizie sull'attività criminale on line che prosegue e si incrementa senza sosta dimostrano come gli incidenti informatici costituiscano oggi per le aziende una grave minaccia.

L'uso intensivo di internet e di tutte le connessioni da parte delle realtà produttive, dei loro collaboratori, dei loro fornitori e dei loro clienti incrementa i possibili obiettivi sensibili al rischio cyber. Il risultato è che il timore da parte delle aziende di subire un attacco è già al secondo posto nella graduatoria dei rischi più temuti dalle imprese, sia nel mondo che in Italia (Fig. 1).

FIGURA 1: GRADUATORIA DEI RISCHI PIÙ TEMUTI DALLE IMPRESE ITALIANE PER IL 2018

POSIZIONE	Rischio	%	Posizione	Trend
1	Danni da interruzione di esercizio	51%	1 (36%)	=
2	**Attacchi cyber**	**38%**	**4 (23%)**	↑
3	Catastrofi naturali	30%	3 (25%)	=
4	Perdita della reputazione o del valore del brand	23%	10 (9%)	↑
5	Incendio, esplosioni	17%	6 (16%)	↑
6	Nuove tecnologie (interconnettività, nanotecnologia, intelligenza artificiale, stampa 3D, droni) **NEW**	16%	-	↑
7	Novità legislative e regolamentari (cambio di governo, sanzioni economiche, protezionismo, Brexit, disintegrazione Eurozona)	14%	7 (14%)	=
8	Sviluppi di mercato (Volatilità, intensificazione della concorrenza, stagnazione/fluttuazione del mercato, fusioni e acquisizioni)	13%	2 (30%)	↓
9	Cambiamento climatico, incremento della variabilità del tempo **NEW**	11%	-	↑
10	Rischi ambientali (es. inquinamento) **NEW**	10%	-	↑

Fonte: Allianz Risk Barometer 2018

Secondo una ricerca svolta da Accenture Security su circa 2000 imprese con fatturato superiore a un milione di dollari a livello mondiale, il 70% di queste ancora non riesce a difendersi adeguatamente e gli incidenti cyber causano danni che possono raggiungere cifre importanti (tabella 1).

TABELLA 1: DANNO MEDIO E MASSIMO PER INCIDENTI CYBER SUBITI DALLE AZIENDE USA NEL 2005-2014 (MILIONI DI €)

TIPO DI INCIDENTE	Danno medio	Danno massimo
Data breach (divulgazione involontaria di dati personali da perdita o furto)	5	486
Compromissione o interruzione dei sistemi IT aziendali	8	85
Violazione volontaria non autorizzata della privacy	9	638
Accessi illeciti ai sistemi informatici	17	604
TOTALE	**7**	**638**

Fonte: Sigma 1/2017, Swiss Re

€

Gli incidenti cyber causano danni che arrivano a centinaia di milioni di euro

I più comuni incidenti cyber e relativi danni

Violazione dati confidenziali (dati propri e di terzi)
Es. furto di segreti commerciali; rivelazione non autorizzata di informazioni sensibili di terzi

- costi per il contenimento del danno
- violazione privacy
- danno reputazionale
- spese legali
- risarcimento danni o multe
- furto di proprietà intellettuale
- responsabilità civile delle alte cariche societarie

Malfunzionamento dei sistemi informatici/rete di comunicazione
Es. manipolazione dei sistemi informatici; attacco al sito web aziendale

- interruzione di esercizio
- risarcimento danni o multe
- danni fisici ai sistemi informatici
- infortunio e morte dei dipendenti
- costi per il contenimento del danno
- danno reputazionale
- responsabilità civile delle alte cariche societarie

Cancellazione o deterioramento di dati
Es. attacco malware, ossia un programma informatico (virus) che compromette il sistema e ruba i dati

- costi per il contenimento del danno
- perdita di dati
- spese legali
- responsabilità prodotti
- responsabilità civile delle alte cariche societarie

Violazione dati confidenziali (dati propri e di terzi)
Es. furto di segreti commerciali; rivelazione non autorizzata di informazioni sensibili di terzi

- interruzione di esercizio
- responsabilità di sicurezza della rete
- spese legali

Crittografia dei dati e furto/ frode finanziaria
Es. attacco ransomware, che limita l'accesso ai dati richiedendo un riscatto

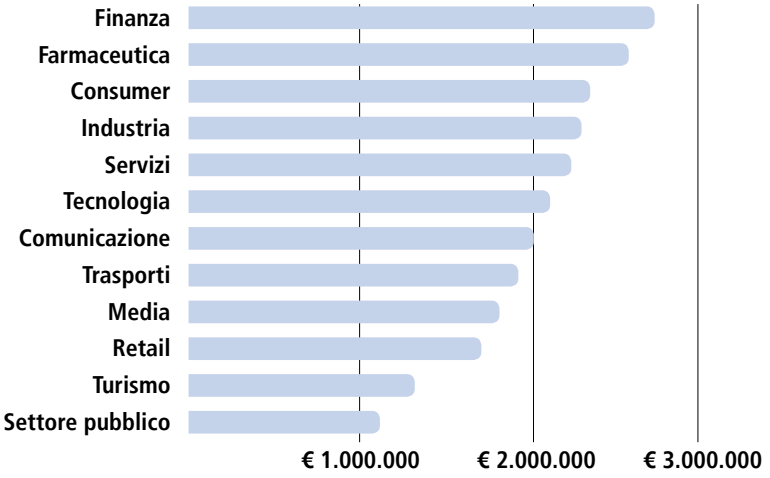
- costi per il contenimento del danno
- riscatto ed estorsione dei dati
- furto/frode finanziaria
- responsabilità civile delle alte cariche societarie

Un modo efficace per comprendere le implicazioni e i possibili danni di un attacco cyber è di confrontarlo con un terremoto che può accadere ovunque e in qualunque momento, può causare danni alle cose, alle persone e può interrompere attività produttive e servizi. Un attacco cyber può causare gli stessi danni ma, a differenza dei terremoti che accadono raramente e quando si verificano interessano un'area limitata, questo può essere frequente ed esteso. Infine, mentre i terremoti non sono provocati dall'uomo e i danni attesi che generano possono in qualche modo essere stimati a seconda del luogo dove si verificano, gli attacchi cyber sono creati quasi sempre dall'uomo e difficilmente possono essere quantificati. Per esempio, dal momento che una stessa piattaforma IT, uno stesso software o uno stesso servizio cloud di un medesimo fornitore sono usati da centinaia o migliaia di utenti, il rischio di subire un attacco in realtà si moltiplica molto facilmente.

Secondo ENISA, l'Agenzia europea per la sicurezza delle reti e dell'informazione, la minaccia più importante registrata nel 2017 è stata quella degli attacchi malware, ossia software che disturbano le operazioni di un computer, rubano informazioni sensibili, violano sistemi informatici o mostrano pubblicità indesiderata danneggiando la reputazione dell'azienda. Seguono gli attacchi via web e il *phishing*, le truffe internet in cui la vittima è convinta impropriamente a fornire dati personali o codici di accesso.

In Italia, i danni da cyber crime nel 2017 ammontano a circa 10 miliardi di euro. Il danno medio è pari a 2 milioni di euro, in aumento del 70% rispetto a tre anni prima. Le realtà più colpite (Fig. 2) appartengono al comparto finanziario, a quello farmaceutico e ai beni di consumo.
Il tempo medio impiegato da un'impresa per capire di essere sotto attacco cyber è di 205 giorni. Ne servono invece 74 per riprendersi.
Secondo un'indagine della Banca d'Italia sulle imprese non finanziarie quasi tutte le aziende hanno adottato misure di prevenzione da rischi informatici ma il 30,3% delle stesse dichiara di avere subito comunque danni nel periodo settembre 2015 - settembre 2016.
E si tratta - secondo l'Istituto - di un dato che sottostima la realtà, perché una percentuale significativa dei casi non viene dichiarata. Infatti AIBA (Associazione italiana broker assicurativi) stima per il 2017 che il 50% delle piccole e medie aziende siano state colpite da un cyber crime per un costo medio di 35.000 euro.

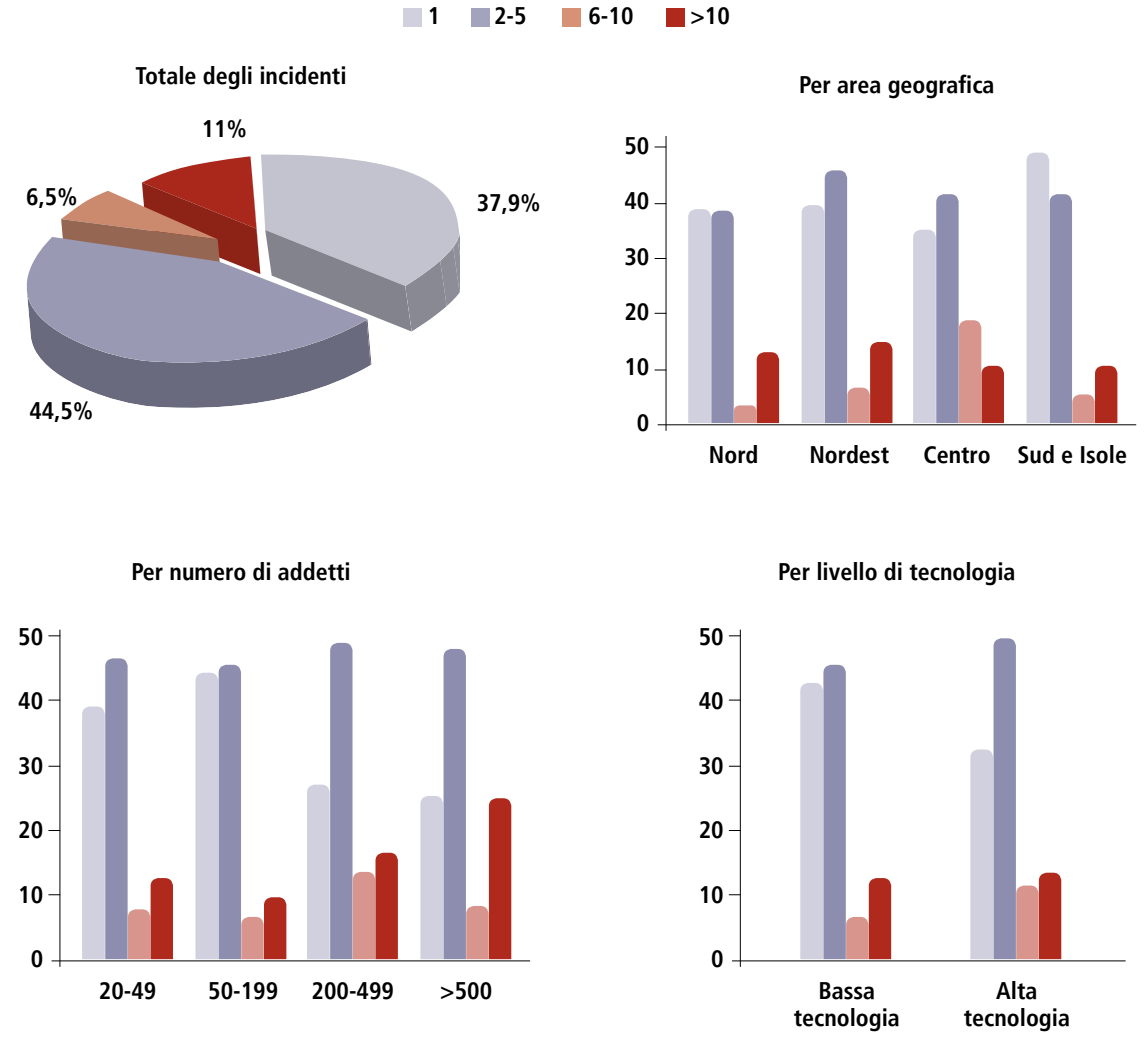
FIGURA 2: DANNO MEDIO ANNUO DA ATTACCHI INFORMATICI ALLE IMPRESE ITALIANE PER SETTORE DI ATTIVITÀ



Le aziende italiane che subiscono danni da attacchi informatici sono tra il 30% e il 50%

Per il resto l'indagine non denota una significativa distinzione dell'esposizione al rischio cyber per area geografica né fra imprese più o meno tecnologiche.
L'unico fattore chiave sembra essere la dimensione della realtà produttiva: più è alto il numero di dipendenti, maggiore è la frequenza di incidenti cyber. Anche se ci sono eccezioni, sono proprio le piccole e medie attività produttive a essere più vulnerabili o perché ancora non del tutto consapevoli del rischio o perché essendo piccole realtà non sono in grado di avere risorse dedicate a gestirlo, per cui delegano spesso all'esterno tutte le funzioni informatiche o di sicurezza.

FIGURA 3: DISTRIBUZIONE DELLE IMPRESE ITALIANE VITTIME DI INCIDENTI CYBER NEL PERIODO SET 2015 - SET 2016



Fonte: Banca d'Italia

LE MISURE DI SICUREZZA E PREVENZIONE: COSA FARE

La risposta in sede europea all'insicurezza informatica è stata innanzitutto la Direttiva 2016/1148 (NIS-Network and Information Security) sulla sicurezza delle reti e dei sistemi informativi che prevede un aumento dei livelli di sicurezza, un incremento della cooperazione tra gli Stati dell'Unione Europea e, per i fornitori di servizi digitali o essenziali, come energia, trasporti, sanità, acqua, nuove misure sulla prevenzione, sulla gestione dei rischi o sulla notifica degli incidenti che possono interrompere la continuità dei servizi. L'Italia ha attuato la Direttiva il 9 maggio 2018 e le nuove norme saranno applicate entro quest'anno.

Inoltre il 25 maggio 2018 è entrato in vigore in tutta Europa il nuovo Regolamento n. 679/2016 (GDPR - General Data Protection Regulation) sulla protezione dei dati personali che, tra l'altro, impone ad un'azienda di comunicare ai propri clienti, entro 72 ore, ogni violazione di dati che comporti un rischio per i diritti e la libertà individuali, pena l'applicazione di sanzioni importanti.

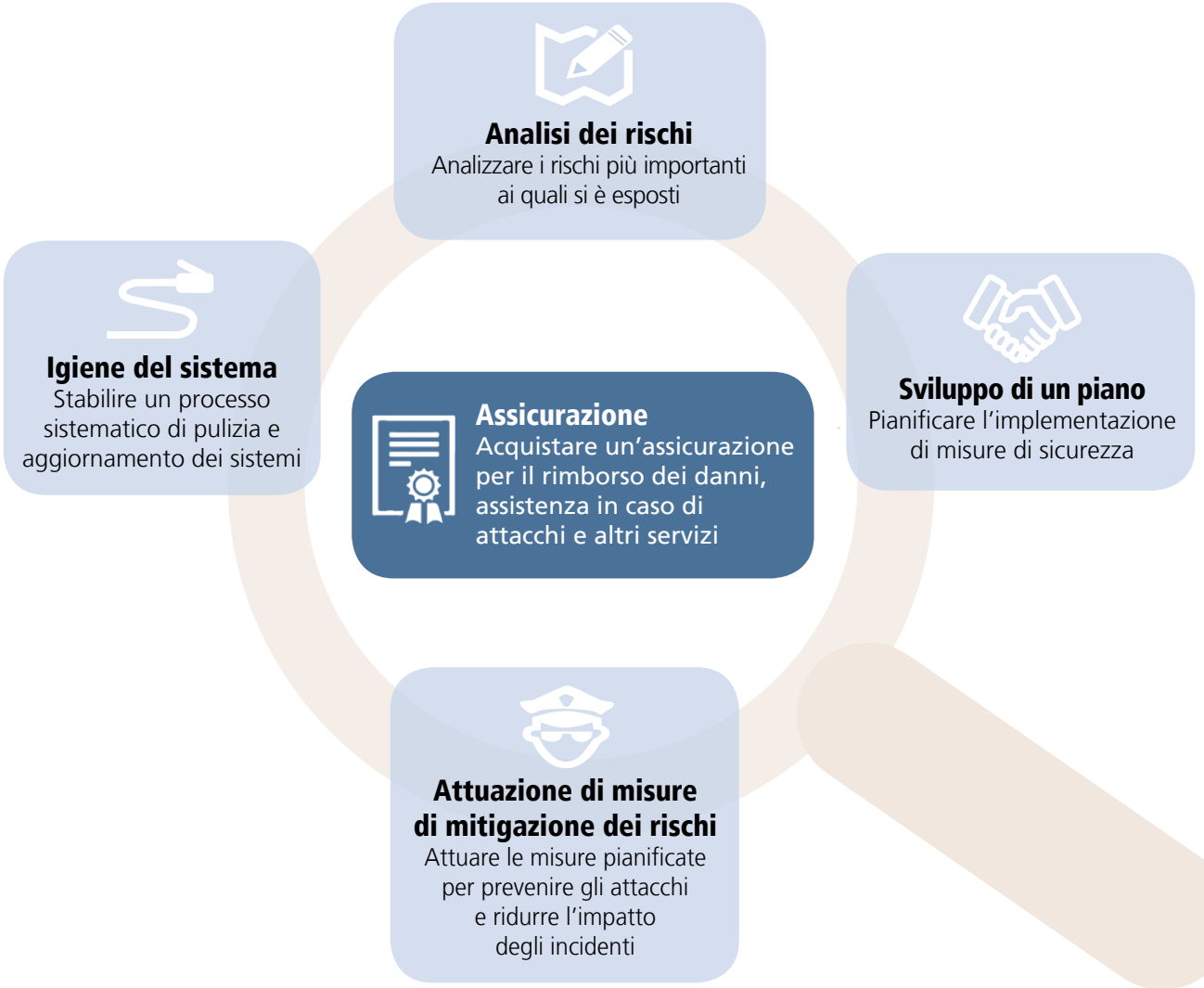
Anche questa Direttiva prevede obblighi sulla continuità operativa e sulla protezione:

- ***aggiornare l'informativa privacy***, il trattamento dei dati personali va gestito ora con maggiore attenzione, ci sono nuove misure, tra l'altro, su tempi e modi di conservazione dei dati per formulare reclami al Garante privacy o sul trasferimento dei dati all'estero;
- ***predisporre una valutazione sulla protezione dati***, quando il trattamento dei dati può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- ***controllare i propri sistemi di sicurezza e implementare misure tecniche e organizzative*** per garantire un livello di protezione e sicurezza adeguato;
- ***valutare la nomina di un responsabile della protezione dei dati***, indipendente, che accompagni l'impresa nell'adeguare la sicurezza del trattamento dei dati e sia tramite con le autorità amministrative in caso di violazioni di sicurezza o richieste di adempimenti.

Al di là delle nuove e importanti norme europee, la sicurezza informatica presuppone innanzitutto la consapevolezza da parte dell'azienda dei rischi che si corrono. Occorre quindi:

- mappare e descrivere i rischi corsi, individuare le attività o le persone che possono essere oggetto di incidenti, le cause di questi, le condizioni che li provocano;
- valutare frequenza, gravità e perdite avvenute o potenziali e prendere in considerazione soluzioni per ridurre i danni, almeno quelli più gravi;
- elaborare un piano per la gestione dei rischi decidendo le misure da adottare e programmando la loro "messa a terra". Nella Fig. 4 si riportano alcune fasi da attuare per una gestione del rischio appropriata, fermo restando che ogni realtà produttiva ha le sue specificità

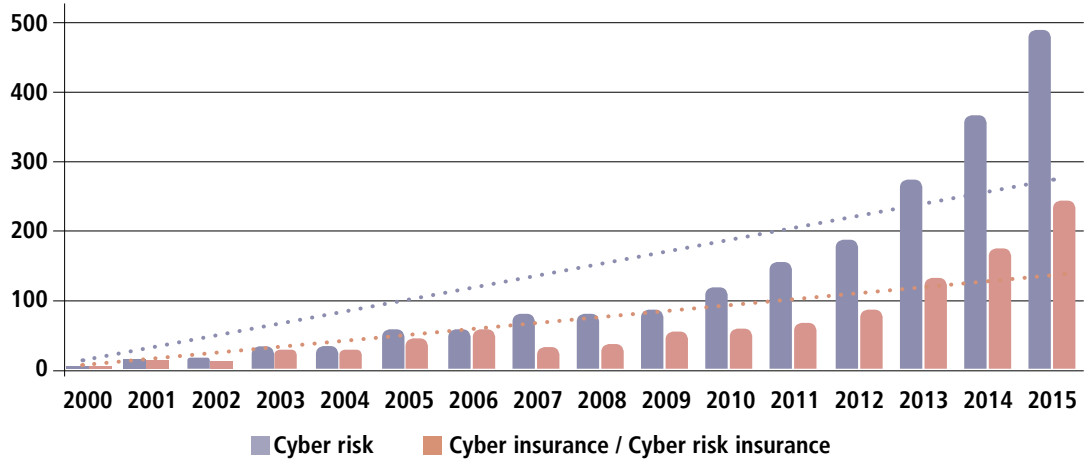
FIGURA 4: LA GESTIONE DEL RISCHIO CYBER



L'ASSICURAZIONE: UNA DELLE POSSIBILI SOLUZIONI

Tra le forme di prevenzione e contenimento del rischio cyber c'è anche l'assicurazione. Spesso, infatti, nei testi al termine "rischio cyber" è associato il termine "assicurazione" (Fig. 5).

FIGURA 5: TESTI CONTENENTI LE PAROLE "CYBER RISK" E "CYBER RISK INSURANCE" O "CYBER INSURANCE"



Fonte: The Geneva Association - testi in Google-scholar

Il mercato assicurativo cyber ha ancora le caratteristiche del mercato poco sviluppato: disponibilità limitata di prodotti assicurativi, clienti potenziali che non comprendono il valore di una copertura che può avere l'assicurazione perché non sono consapevoli della loro esposizione al rischio e di quali danni questo può causare. Eppure assicurare la propria realtà produttiva la protegge da imprevisti che possono comprometterne la reputazione, i risultati o la stessa sopravvivenza.
Si può trovare protezione con prodotti assicurativi specializzati per il rischio cyber che coprono i danni subiti e quelli provocati a terzi - per esempio, i clienti - per violazione di dati sensibili o disservizi. Le sei "garanzie-chiave" di una copertura cyber sono le seguenti:

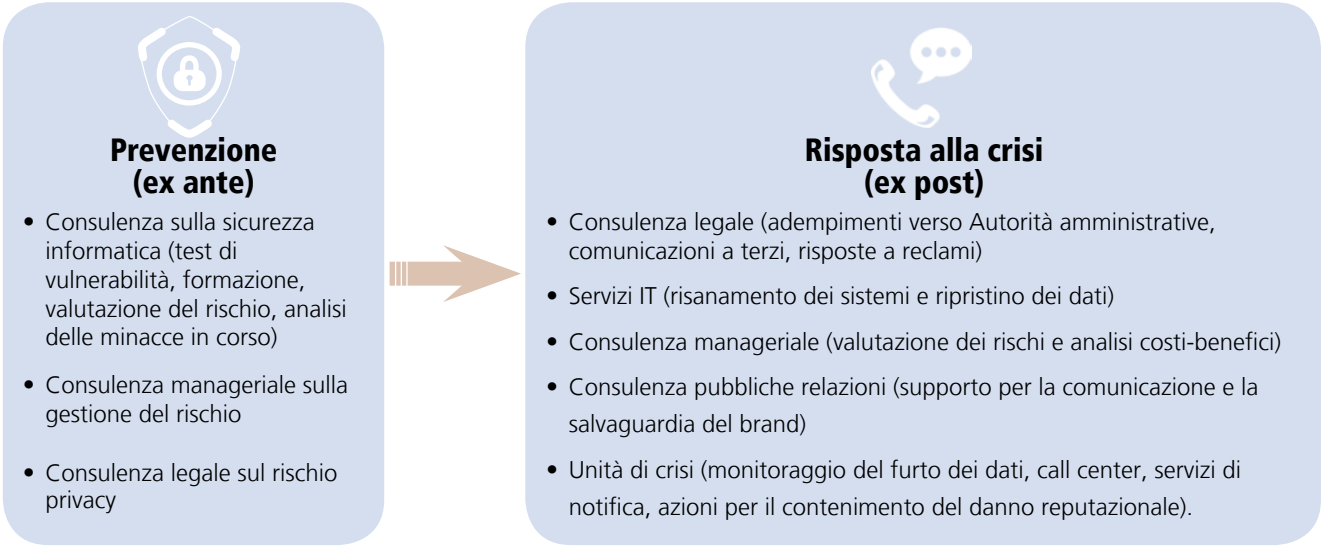
FIGURA 6: GARANZIE PRINCIPALI DELL'ASSICURAZIONE CYBER

Inoltre le polizze possono abbinare alle garanzie cyber, su scelta del cliente, altri tipi di garanzie:

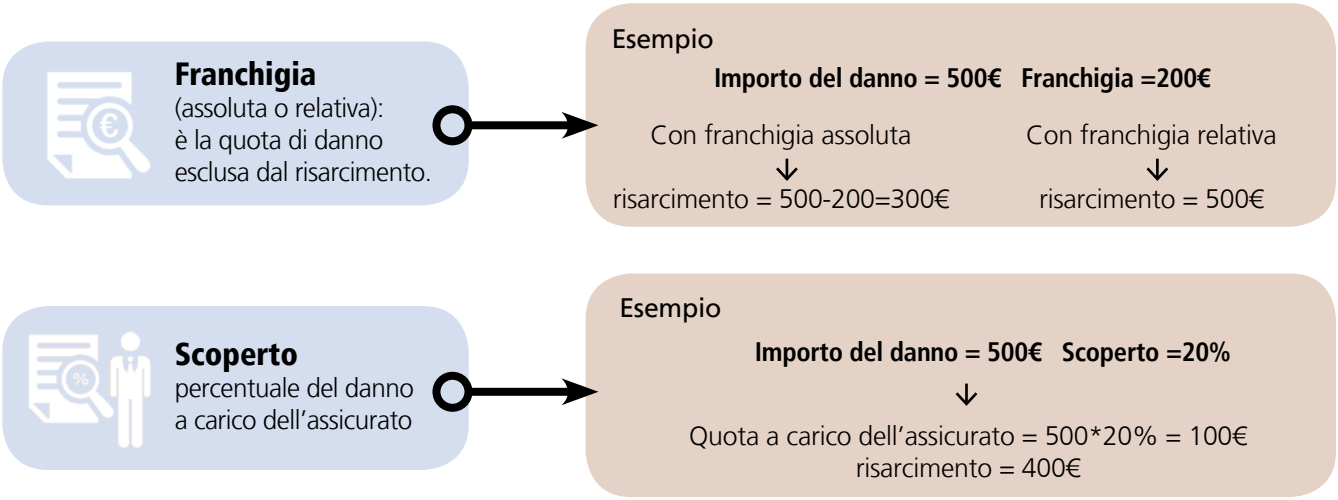
FIGURA 7: ALTRE POSSIBILI GARANZIE DELL'ASSICURAZIONE CYBER

Infine quello che contraddistingue alcune polizze cyber è la presenza di servizi che rendono il prodotto assicurativo un pacchetto completo per la gestione del rischio (cfr. Fig. 8), sia in termini di prevenzione (gestione del rischio ex ante) che in termini di risposta alla crisi a seguito dell'incidente (gestione del rischio ex post).

FIGURA 8: SERVIZI AGGIUNTIVI DI UN'ASSICURAZIONE CYBER



Per contenere il prezzo dell'assicurazione le compagnie prevedono dei limiti ai risarcimenti come:



Massimale
importo massimo del risarcimento.

Esempio

Importo del danno = 500€

Con massimale = 1000€	Con massimale = 300€
↓	↓
risarcimento = 500€	risarcimento = 300€

Esclusioni
casi in cui la copertura non è valida.

Esempio
- danni alle persone o agli animali;
- danni causati dal mancato rispetto di contratti o accordi;
- danni causati da pratiche commerciali scorrette;
- danni causati da comportamenti illegali, commessi dall'azienda in modo premeditato;
- danni causati da inquinamento dell'aria, dell'acqua o del suolo, da operazioni belliche o da atti di terrorismo;
- danni causati da guasti a centrali che forniscono servizi di alimentazione (energia, telecomunicazione) all'azienda.

È molto importante, anche nelle coperture cyber, verificare i limiti previsti.

L'azienda dovrebbe valutare con attenzione quali incidenti comprometterebbero la sua operatività e decidere per quali rischi assicurarsi. In questo è fondamentale che l'assicuratore assista l'azienda nel comprendere i pericoli ai quali è esposta e nell'individuare le possibili soluzioni.
Il prezzo dell'assicurazione non è uguale per tutti. Come per gli altri rischi anche per il rischio cyber dipende dalla frequenza con cui l'incidente si può ripetere e dalla sua gravità: alcuni rari ma molto gravi e altri più frequenti, ma di minore impatto. L'assicurazione stima sulla base di questi due elementi il costo della copertura. Quindi il prezzo può dipendere dagli attacchi che l'azienda ha già subito, da quali misure di sicurezza e sistemi informatici adotta o da quali dati tratta. Per il resto il prezzo dipende essenzialmente dalla dimensione o dal fatturato dell'impresa.

È utile sapere poi che molti studi, tra i quali uno dell'ANIA svolto in collaborazione con CERVED nel 2014, dimostrano che le imprese più assicurate hanno anche un migliore accesso al credito sia dal punto di vista delle condizioni del finanziamento sia da quello del numero di istituti disposti a concederlo.
Data la natura potenzialmente "catastrofale" e attendendosi una sua crescita significativa nel prossimo futuro, secondo l'Agenzia di rating Moody's, il rischio cyber avrà sempre più peso rispetto alle misure di prevenzione da adottare e nelle valutazioni del merito creditizio delle aziende, specialmente di quelle che operano nei servizi essenziali.

Perché la copertura sia adeguata alle caratteristiche specifiche dell'azienda, è necessario che quest'ultima accetti di condividere alcune informazioni sulla propria attività.
La resistenza a rendere pubblici i dati per paura di compromettere la propria sicurezza aziendale è un ostacolo da superare. In questo senso, al di là dell'atteggiamento della singola realtà produttiva, anche le associazioni rappresentative possono fare molto, per esempio raccogliere dati in modo anonimo per consentire la stima del costo dell'assicurazione in base alle caratteristiche della singola realtà produttiva. Così come possono contribuire le istituzioni mettendo a disposizione le informazioni sugli incidenti informatici, anche alla luce della nuova normativa sulla protezione dei dati al fine di permettere lo sviluppo di un mercato assicurativo efficiente.

Il rischio cyber: conoscerlo di più per proteggersi meglio

BIBLIOGRAFIA

- *ASSINEWS 294* - Febbraio 2018
- *Allianz Risk barometer 2018* - Allianz Global Corporate & Specialty (AGCS), Gennaio 2018
- *Security Index* – Accenture, Aprile 2017
- *Sigma: Cyber getting to grips with a complex risk* – Swissre, Gennaio 2017
- *Enhancing the Role of Insurance in Cyber Risk Management* – OECD, Novembre 2017
- *Questioni di Economia e Finanza: Cyber-attacks: preliminary evidence from the Bank of Italy's business surveys* – Banca d'Italia, Febbraio 2017
- *Advancing Cyber Resilience: Principles and Tools for Boards* – World Economic Forum, Gennaio 2017
- *Achieving Cyber Resilience* – AIG, 2017
- *Relazione 2017 sulla politica dell'informazione per la sicurezza* - Presidenza del Consiglio dei Ministri, Febbraio 2018
- *Supporting an effective cyber insurance market* - OECD, Maggio 2017
- *Insuring cyber risk* – Federation Francaise de l'Assurance (FFA), Gennaio 2018
- A*dvancing Cyber Resilience Principles and Tools for Boards* – World Economic Forum, Gennaio 2017
- *Unleashing the Potential of the Cyber Insurance Market, CONFERENCE OUTCOMES* – OECD, Febbraio 2018
- *Ten Key Questions on Cyber Risk and Cyber Risk Insurance* – The Geneva Association, Novembre 2016
- *Cyber insurance as a Risk Mitigation Strategy* – The Geneva Association, Aprile 2018
- *Making sense of cyber Insurance: a guide for SMEs* – ABI, Association of British Insurers, Maggio 2016
- *Coperture assicurative e probabilità di default delle PMI* – ANIA-CERVED, Settembre 2014
- *Cyber risk of growing importance to credit analysis* – Moody's, November 2015

Ania

Associazione Nazionale
fra le Imprese Assicuratrici