Allianz Risk Barometer 2019

Executive Summary

La tecnologia sta generando nuovi scenari di rischio e modelli di business. I rischi tradizionali come le Catastrofi naturali continuano a rappresentare un pericolo, mentre evolvono costantemente altre minacce come i Rischi Cyber, per la prima volta al vertice dell'Allianz Risk Barometer a pari merito con l'Interruzione di attività, e il Danno reputazionale.

L'interruzione di attività (BI) è per il settimo anno consecutivo la principale minaccia percepita dalle aziende (37% delle risposte). Secondo AGCS, l'indennizzo medio di un sinistro danni indiretti property ammonta a 3,1 milioni € (3,4 milioni $). Si tratta di oltre un terzo (39%) in più della corrispondente perdita media dei danni materiali diretti (2,2 milioni di €), con un totale molto superiore a quello di 5 anni fa. Le perdite derivanti dagli eventi più importanti possono essere di centinaia di milioni o superiori.

Le aziende si trovano ad affrontare un numero crescente di scenari di **Interruzione di attività**. Molti di essi possono verificarsi senza danni diretti ma con perdite elevate. Eventi come incidenti ai sistemi IT di base, il richiamo dei prodotti o mancanza di qualità, terrorismo, violenza politica o disordini, e inquinamento ambientale possono portare le aziende a un punto morto, il che significa che le stesse potrebbero non essere in grado di fornire prodotti e servizi con un impatto devastante sui ricavi. Ad esempio, dopo 4 fine settimana di proteste in Francia alla fine del 2018 i commercianti hanno perso circa 1 miliardo di € (1,1 miliardi di $).[1] Nell'incertezza del panorama politico odierno, il cambiamento legislativo, come la prevista uscita del Regno Unito dall'Unione Europea (Brexit) nel 2019, rappresenta una potenziale minaccia per la BI con possibili interruzioni della supply chain.

L'**Interruzione di attività** è affiancata per la prima volta in cima alla classifica dai **Rischi informatici** (37%)[2]. Secondo AGCS, anche la perdita media per un incidente informatico è di poco più di 2 milioni di € [3] (2,3 milioni di $) rispetto a quasi 1,5 milioni di € per un incendio/esplosione, mentre le perdite per eventi importanti possono ammontare a centinaia di milioni o più. Sempre più spesso gli incidenti informatici provocano perdite di danni indiretti. Gli intervistati classificano il cyber come il fattore più temuto di attivazione della BI, dato che le risorse primarie di molte aziende possono spesso essere dati, piattaforme di servizi o gruppi di clienti o fornitori.

I sinistri di interruzione dell'attività sono stati la conseguenza degli attacchi malware **WannaCry** e **NotPetya** nel 2017, che hanno colpito le aziende di spedizione, logistica e produzione. Le Compagnie assicurative hanno visto aumentare le richieste di risarcimento per danni indiretti a seguito di incidenti informatici per importi superiori a 100 milioni di $. Molti danni sono il risultato di errori tecnici o umani piuttosto che di atti dolosi - l'analisi condotta dall'autorità di regolamentazione dei servizi finanziari del Regno Unito ha rivelato un aumento del 138% dei guasti tecnologici in un anno, ma solo il 18% degli incidenti segnalati sono stati attacchi informatici[4]. I black out informatici rappresentano un rischio significativo. Gli sbalzi di tensione o i problemi di migrazioni di piattaforme IT possono costare centinaia di milioni di euro. La dipendenza dai fornitori di servizi IT - come i servizi cloud, le piattaforme di prenotazione online e i sistemi legati alla supply chain - comporta anche potenziali esposizioni a interruzioni per motivi indiretti (CBI). Un'anomalia software che ha colpito nel 2018 il fornitore di apparecchiature di rete Ericsson, ha interrotto i servizi per milioni di clienti di telefonia mobile in Europa e in Giappone[5]. Nel 2017, un'interruzione di quattro ore della divisione di cloud computing AWS di Amazon, ha avuto un impatto sui servizi internet, siti web e altre attività commerciali. Come risultato le aziende hanno perso circa 150 milioni di dollari[6]. Le interruzioni più lunghe potrebbero portare a perdite molto più vicine al miliardo di dollari.

La criminalità informatica costa circa 600 miliardi di $ all'anno[7] rispetto a 445 miliardi di $ del 2014. A fronte di una perdita economica media decennale per catastrofi naturali di circa 200 miliardi di $, il triplo. Esiste anche una crescente minaccia da parte degli Stati sovrani, che utilizzano la tecnologia per sottrarre dati preziosi e segreti commerciali, con implicazioni per le imprese.

---

1 BBC News, 9 dicembre 2018, Yellow vest protests 'economic catastrophe for France

2 BI e incidenti informatici ammontano al 37%. La BI ha ricevuto più risposte per numero - da 1.078 a 1.052.

3 Il valore medio degli indennizzi informatici è di € 2.007.653 sulla base di 115 sinistri del settore assicurativo tra il 2013 e il 2018.

4 The Financial Conduct Authority, November 27, 2018, Cyber and technology resilience in UK financial services

5 Reuters, 6 dicembre 2018, Ericsson sorry for software glitch that hits mobile services in Britain and Japan

6 Guidewire Cyence Risk Analytics, MMC Cyber Handbook 2018, Evolution of Cyber Risks Quantifying Systemic Exposures

7 Center for Strategic and International Studies, Economic Impact of Cybercrime – No Slowing Down

L'impatto delle violazioni dei mega dati, degli scandali sulla privacy e l'introduzione del regolamento generale dell'Unione europea sulla protezione dei dati - che ha anche ispirato norme più severe in materia di privacy e la minaccia di pesanti sanzioni pecuniarie altrove - sono anch'essi fonte di preoccupazione per le imprese. È sempre più probabile che gli incidenti informatici siano all'origine di controversie, comprese le “class action”.

Ogni azienda deve assumere una posizione di sicurezza informatica adeguata alle dimensioni, alle operazioni e al profilo di rischio, e investire in soluzioni tecnologiche di sicurezza, meccanismi di backup adeguati e formazione del personale. Quest'ultimo aspetto è altrettanto importante, soprattutto per le piccole e medie imprese, per le quali la consapevolezza della crescente minaccia informatica e del suo legame con la perdita di reputazione è una preoccupazione crescente.

Grandi eventi come gli uragani Michael e Florence in Nord America, il tifone Jebi in Giappone e altri incendi in California hanno provocato circa 146 miliardi di $[8] di perdite economiche causate da **Catastrofi naturali** (3° 28%) nel 2018, dopo un anno di perdite record nel 2017. Gli intervistati sono preoccupati che le attività recenti possano essere causa di crescenti perdite finanziarie e di ripercussioni sui mercati, così che il **Cambiamento climatico** (8° 13%) raggiunge la sua posizione più alta di sempre. Oltre ai danni e alle implicazioni materiali, i cambiamenti climatici avranno probabilmente un importante impatto per la regolamentazione e la responsabilità. I rigidi obiettivi nelle emissioni stanno già modificando l’operatività di alcuni settori come l'aviazione e il trasporto marittimo. L'aumento degli obblighi di comunicazione e di informazione aumenterà l'esposizione delle società, degli amministratori e dei funzionari.

Le imprese sono più preoccupate del **Cambiamento dello scenario legislativo e regolamentare** (4° 27%) rispetto a 12 mesi fa, mentre le guerre commerciali, le tariffe e la continua situazione di incertezza sulla **Brexit**, hanno acuito i timori rispetto alla resilienza delle supply chains. Il **Cambiamento nei mercati** (5° 23%) rimane un rischio “top five” dopo che il 2018 è stato caratterizzato dall’aumento della volatilità, delle divergenze e delle sorprese da record. L’impatto dei danni derivanti da **Incendi ed esplosioni** (6° 19%) è una preoccupazione costante. Secondo AGCS, negli ultimi cinque anni gli incendi (esclusi quelli boschivi) hanno causato perdite assicurative per oltre 14 miliardi di € (15,9 miliardi di $), rendendoli la principale causa di perdite per le imprese.

Le nuove tecnologie (7° 19%)[9] offrono alle imprese grandi opportunità, compresi nuovi modi per gestire il rischio. Tuttavia, con l'aumento del numero di macchine connesse, si pongono anche domande sulla sicurezza, la protezione dei dati, la continuità operativa e la responsabilità civile, nonché il rischio di guasti alle infrastrutture critiche. Conseguenze inaspettate continuano a materializzarsi, come ad esempio i droni che hanno provocato la cancellazione di circa 1.000 voli all'aeroporto britannico di Gatwick nel dicembre 2018. Nel frattempo, i richiami di prodotti, gli incidenti informatici e la condotta dei dirigenti hanno contaminato la reputazione delle società negli ultimi anni, colpendo compagnie aeree, case automobilistiche, banche e organizzazioni di beneficenza; ciò significa che la protezione dal **Danno reputazione o d’immagine** (9° 13%) diventa sempre più importante, soprattutto nell'era dei social media in cui le crisi si diffondono rapidamente. La **Carenza di manodopera qualificata** (10° 9%) appare per la prima volta tra i primi 10 rischi a livello mondiale, e il cambiamento demografico e la Brexit hanno contribuito alla sua crescita.

Un elenco così lungo e diversificato di scenari richiede nuove soluzioni di gestione del rischio, strumenti e partnership per controllare e mitigare i loro potenziali impatti. L'assicurazione fornisce sempre più spesso un'assistenza tangibile ai rischi immateriali. La copertura dei rischi informatici sta diventando una parte importante in risposta agli incidenti, fornendo alle aziende l'accesso a servizi di consulenza specialistica che possono aiutare a combattere e a prepararsi meglio agli eventi. L'assicurazione Cyber per la BI può ridurre la perdita di ricavi e costi derivanti da indisponibilità di dati e sistemi a causa di hacking, guasti tecnici o errori dei dipendenti. L’assicurazione BI “non-damage” indennizza un'azienda per la perdita di ricavi a causa di un evento negativo, come ad esempio proteste o sommosse. L'assicurazione del rischio reputazionale fornisce costi di consulenza e di risposta in caso di crisi.

Le nuove tecnologie stanno inoltre potenziando l'analisi dei rischi. Assicuratori come AGCS ora utilizzano l'analisi semantica per comprendere meglio il rischio della supply chain, i droni per valutare rapidamente i danni da catastrofe, e stanno collaborando con aziende informatiche per identificare i rischi di contenzioso di nuova generazione. In un mondo sempre più interconnesso, i dati provenienti da dispositivi, fabbriche e supply chain offriranno l'opportunità di una migliore valutazione dei rischi attraverso indicatori predittivi e soluzioni più flessibili, personalizzate e tempestive, con l'obiettivo finale di comprendere e gestire i rischi più rapidamente per prevenire le perdite prima che si verifichino.

8 Swiss Re, 18 dicembre 2018

9 Incendi, esplosioni e nuove tecnologie ammontano al 19%. Incendi e esplosioni hanno ricevuto più risposte