Per gentile concessione di Clusit

RAPPORTO CLUSIT 2016

Focus On

"Assicurare il rischio informatico"

A cura di

A. Pennasilico – Obiectivo

C. Burei – Margas

R. Scalici – Chubb

Prendi visione del contenuto su http://clusit.it/rapportoclusit/

Richiedi il report completo a rapporti@clusit.it

Assicurare il Rischio Informatico

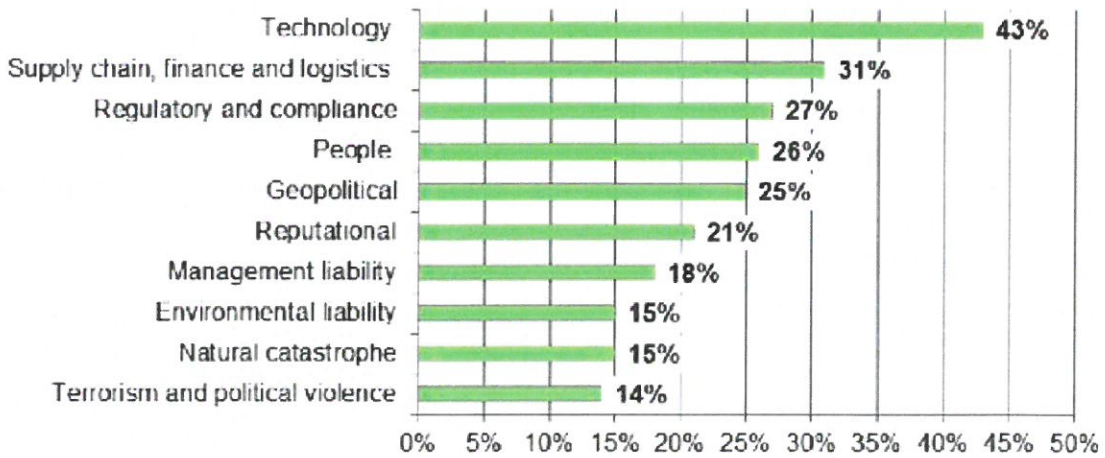
A cura di Alessio Pennasilico, Cesare Burei e Riccardo Scalici

Trasferire il rischio: questa, tra le diverse possibili azioni previste nella gestione di un rischio, è quella che tradizionalmente crea più incertezze quando si parla di sicurezza delle informazioni. Altre funzioni aziendali hanno a disposizione informazioni, know how e strumenti che hanno una lunga storia alle spalle. Assicurare i beni del magazzino o l'edificio da rischi quali furto o incendio è una delle azioni che le aziende compiono da ben prima dell'apparizione degli strumenti informatici. Stimare l'impatto che questi avvenimenti possono comportare per la gestione delle informazioni e di conseguenza per il business aziendale, è invece molto diverso.

I rischi, infatti, non possono e non devono essere catalogati per *banali colori* come troppo speso si riscontra nei file excel che si trovano compilati nelle aziende. Non esiste un rischio "alto-3-rosso": esiste un rischio da € 3.000.000, € 30.000.000 o € 300.000.000. Ed esistono le relative contromisure.

Calcolare i rischi su base economica è indispensabile per poterli raccontare in modo comprensibile alla Direzione, permettendo di prendere le decisioni strategiche corrette. Diventa poi indispensabile quantificare il rischio per poter discutere con il proprio assicuratore, ad esempio, il massimale della polizza, nel caso in cui si decida di trasferire il rischio.

In questo ultimo caso è bene fare molta attenzione a cosa si assicura e per quali evenienze. Per questo, conoscere le ratio, i contratti e gli algoritmi utilizzati dalle assicurazioni diventa fondamentale. Quasi tutte le aziende posseggono una polizza incendio. Se a bruciare, però, è la sala server, vedersi rifondere il mero valore dell'hardware sarebbe ottenere un indennizzo sul danno subito più lieve. E come assicurare un furto di dati? Come stimare la differenza tra dati finiti in mano ad un concorrente e dati pubblicati su Internet, come sempre più spesso accade? E un attacco DDoS al proprio sito come si assicura?



I rischi per il Business che attualmente preoccupano di più in Europa, Middle East ed Africa. Fonte: ACE Group

Dalla polizza "tradizionale" alla Polizza Cyber

La pervasività delle tecnologie ICT e di Internet, di fatto cervello, sistema cardio-vascolare e linfatico delle aziende, rende necessaria un'attenta rilettura delle polizze tradizionali (All Risk, Incendi, Trasporti...) e la loro integrazione ragionata con le Polizze Cyber. Infatti, una polizza adeguata ai tempi, deve prevedere coperture in ambito materiale e immateriale, ovvero tener conto di rischi che si riferiscono al livello fisico come a quello logico e ai loro effetti. Da non dimenticare il fatto che causa ed effetto (o effetto dell'effetto) possono essere alternativamente di natura "analogica" o "digitale".
Le polizze Cyber presenti oggi sul mercato italiano sono poche e sono piuttosto diverse tra loro: per linguaggio, strutturazione ed ambito d'azione.

Tipicamente ci troveremo davanti ad una serie di sezioni, attivabili o meno, che prenderanno in considerazione:

- **danni** occorsi ai **beni** ICT (macchine) e ai **dati** propri o di Terzi;
- danni legati alla **violazione della Privacy** (dati personali e/o commerciali) propria o di Terzi;
- danni causati dal **crimine informatico** e quelli **da guasto ed errore umano** (di dipendente o Terzi);
- danni che impattano **sull'attività aziendale** (Interruzione di esercizio, richieste di risarcimento da parte di terzi).

Risarcire una serie di **costi** connessi a questi danni, non è sempre previsto dalle polizze tradizionali.
Compreso cos'è il rischio *cyber* e che esso può essere analizzato, mitigato e infine trasferito, e definita la possibilità di coprire i danni e costi propri (*First Party*) o quelli di terzi (*Third Party*), può essere utile comprendere un po' meglio le **tipologie di danni e costi** per decidere se possiamo aver bisogno di una polizza *cyber* e quali caratteristiche questa deve avere per tutelare il mio *business*.

I cyber-danni

Avvalendoci della terminologia e delle definizioni tratte dalle polizze tradizionali, per calarci nel mondo dei danni *cyber*, possiamo distinguere tre grandi famiglie di danni:

1) Danni materiali diretti

Riguardano i danni (distruzione parziale o totale, furto) subiti da beni materiali (un server, la fibra ottica, i PC, un cellulare o altro *device* elettronico) e direttamente causati dall'evento che sarà normalmente di natura "analogica" o tradizionale (incendio, terremoto, fulmine, furto, atto maldestro o doloso, etc.); per la loro natura essi rientrano già nella polizza Incendio, nella polizza Trasporti, nella polizza *All Risks* (che proprio "tutti i rischi" non copre)... e naturalmente nella Polizza storicamente definita "Elettronica". **I danni materiali e diretti possono anche non essere previsti nella Polizza Cyber,** se ho provveduto alla corretta strutturazione delle coperture assicurative tradizionali.

2) Danni materiali indiretti (o consequenziali)

Si tratta ugualmente di danni a beni materiali, ma conseguenza di danni diretti: per esempio, un fenomeno elettrico che abbia danneggiato una scheda, il cui malfunzionamento danneggi a sua volta la macchina di produzione da essa controllata**. I danni materiali indiretti possono rientrare sia nelle polizze tradizionali che nella Cyber, ma vanno esplicitamente inclusi.**

3) Danni immateriali diretti e indiretti

Sono tutti quelli che non riguardano la materialità delle cose assicurate e che sono **conseguenza** di un evento garantito in polizza, anche di tipo *Cyber*.

L'evento dannoso distrugge, compromette l'integrità di un software e/o l'insieme logico di informazioni – ovvero rende indisponibili i miei dati aziendali. Esempi di questa categoria possono essere l'incendio che brucia il server con il suo contenuto informativo, l'involontaria cancellazione di un *database* clienti o ordini, l'azione erronea - anche colposa - da parte di un dipendente addetto alla gestione informatica, l'azione di un *virus* o *malware*.

Le Polizze Cyber risarciscono certamente i costi sostenuti per la sostituzione del software e le operazioni di ripristino o ricostruzione dei dati. Ma se questo non fosse possibile? Chi mi risarcisce il valore del dato perduto?

Quantificare il valore di un database è un'operazione di una certa complessità. In questo senso una **preventiva analisi degli *asset* immaterial**i, l'adozione documentata di tecnologie/procedure per circoscrivere, valorizzare e proteggere quel bene immateriale ed una accurata analisi patrimoniale renderebbe possibile una valorizzazione dell'eventuale danno alla parte logica e dunque la **adeguata personalizzazione della polizza cyber** in ottica di una mitigazione il più efficace possibile del danno subito.

Va ricordato che l'insieme dei danni materiali e immateriali si traduce tipicamente nell'impossibilità di proseguire la normale attività produttiva (informatica e non) per tutto il periodo necessario alla ricostruzione/ripristino dell'infrastruttura ICT, dei software o dei dati. Per questo si annoverano nella categoria dei Danni Immateriali Indiretti anche i **danni da interruzione di esercizio** o *Business Interruption* e cioè la perdita di quote di mercato nel periodo di indennizzo stabilito in polizza, le mancate vendite, la riduzione dell'utile. Su questi danni, non marginali, si innestano **anche maggiori costi per la ripresa dell'attività** o **la persistenza di costi insopprimibili come leasing e stipendi**. Il tutto, se preventivamente analizzato, è assicurativamente trasferibile. Da notare che in Italia le Polizze Danni da Interruzione di Esercizio vengono sottoscritte da appena il 15 % dei titolari di polizze All Risks ed incendio che ad oggi non comprendono gli eventi *cyber*. C'è da augurarsi che l'omonima sezione delle Polizze *Cyber* goda di maggior attenzione.

Dai danni ai costi

Alle classi di danni precedentemente nominate sono intrinsecamente connessi costi e spese di vario genere volte ad indagare le cause, le eventuali responsabilità e a ripristinare lo stato dell'arte; costi che ci aspettiamo siano rimborsati dalla nostra polizza assicurativa, perché è ad essa che appunto abbiamo cercato di trasferire i nostri rischi.

È opportuno ricordare qui, che:

a) la normativa italiana vieta espressamente il rimborso di multe, ammende e sanzioni amministrative. Così può non essere in altri paesi soggetti a differenti legislazioni.

b) certi assicuratori indicano esplicitamente la **conformità alle norme vigenti** (per esempio alla Legge sulla Privacy) e il raggiungimento di **livelli minimi di sicurezza** (tecnologica, procedurale o di in-formazione del personale) anche documentati da piani di *disaster recovery e business continuity*, quali pre-requisiti per la assicurabilità e la liquidabilità. Altri assicuratori intervengono direttamente con propri tecnici per offrire una polizza il più adeguata possibile alle esigenze aziendali.

Vediamo alcuni **esempi di costi o spese** tratte da diverse polizze *cyber* e quelli afferenti in particolare alla sezione/estensione di polizza **Danni Indiretti o *Business Interruption* (BI)**:

Costi tipicamente compresi e rimborsati	Costi tipicamente connessi a *Business Interruption*
Costi per Consulenza	Canoni di affitto
Consulenza di crisi	Canoni leasing
Consulenza per Pubbliche Relazioni	Stipendi dei dipendenti
Consulente di Reazione	Costi per straordinari dei dipendenti
Costi di Difesa	Spese di manodopera legate al ricorso a personale aggiuntivo
Costi di risposta	Impiego di metodi di lavorazione o di produzione alternativi
Spese per Pubbliche Relazioni	Extracosti per lavorazioni/elaborazioni presso Terzi
Costi (spese) per ripristino (dei dati)	
Servizi di pronto intervento informatico	
Spese di Gestione della Crisi	

continua >

Costi tipicamente compresi e rimborsati	Costi tipicamente connessi a *Business Interruption*
Costi di disinstallazione e reinstallazione dei beni assicurati	
Spese per il ricorso a società di servizio esterne	
Spese per il reperimento rapido di materiali	
Spese di guardiania e conservazione dei beni assicurati	
Spese di Ripristino del Sistema Informatico della Società allo stesso livello di funzionalità che esisteva prima di tale Evento di Interruzione dell'Attività; e/o per Ripristinare tecnicamente, recuperare o reinstallare dati o programmi informatici, compreso il costo di acquisto di una licenza software necessaria per riprodurre tali Dati o Programmi Informatici.	

Nel caso specifico della sezione *Business Interruption* ci si occupa di **indennizzare la Perdita di Profitto Lordo** dovuta alla **Riduzione del Volume di Affari** rispetto a quello di riferimento, e a ristorare l'assicurato delle **spese supplementari sostenute al solo scopo di evitare o contenere la riduzione del Volume di Affari** che si sarebbe verificata a causa del Sinistro.

Cyber-Sinistro, quanto mi costi? Esempi tratti dal mondo reale

Nei casi presi in considerazione e forniti dalle Assicurazioni, vengono esplicitati alcuni parametri considerati significativi: la Causa (Informatica, Errore Umano, Dolosa, ...), il Tempo di ripristino (parziale o totale dell'operatività di SW, Sistemi, Macchine o dipendenti), i Costi (di ripristino), le Perdite di Profitto e ove possibile la Stima della Perdita di Quote di Mercato relative al periodo d'indennizzo. Ove è indicato: "non risarcibile" si intende che la garanzia non è stata acquistata o perché elemento indicato nelle esclusioni. Altrove è indicato "non risarcibile per sottoassicurazione" ovvero che l'importo assicurato è inferiore al danno subito. Riguardo alla Quota Perdita di mercato (p.es: da danno reputazionale), ove stimabile, si intende che non è risarcibile. Si osserva che frequentemente, per inesperienza, gli assicurati sottostimano ampiamente i Tempi di Ripristino e l'entità del danno.

- **Infezione da Virus nel settore: GDO**; Tempo di ripristino: 10 giorni; costi straordinari (solo rete UE): 0,5Milioni €; perdite di profitto risarcite: 0,6 Milioni e; perdita di mercato stimata massimo 7%
- **Errori dello staff IT Settore: TLC**; Tempo di ripristino: 85 giorni (migliaia di server della Rete); costi straordinari: 1 Milione €; perdite di profitto: non risarcibili perché escluse (stimate 55 milioni €).
- **Errori del personale su macchinario industriale nel settore: Industria**; Tempo di ripristino: 70 giorni; riparazione robot: 20% valore della macchina; costi straordinari: 0,3 Milioni €); perdite di profitto (stimate 2 milioni €), ma non liquidate perché non assicurate.

- **Cyber attack su impianti ancillari datacenter nel settore: Gambling**; Tempo di ripristino: 87 giorni (80 per tempi di ricerca); riparazione SW 85.000 €; perdite di profitto su rete 5.000 negozi (25.000 macchine): 14 Milioni €, risarciti 5 M€ per sottoassicurazione.
- **Logic Bomb nel sistema principale nel settore: Finanziario/Assicurativo**; Tempo di ripristino: 88 giorni parziale; riparazione SW 54.000€; perdita da frode informatica (distrazione fondi): 10 milioni€, non risarciti perché la frode non era assicurata, recupero impossibile.
- **Frode informatica nel settore TLC**; Tempo di ripristino 5 giorni; perdita monetaria da frode 1,5 milioni € (distrazione traffico telefonico), risarcimento 50.000 € per sottoassicurazione, recupero impossibile.
- **Data Breach con frode settore: Event Management**; Tempo di ripristino 3 giorni; perdita da concorrenza sleale: 40% del fatturato gare; nessun risarcimento *Data Base* e BI perché assicurati solo su hardware e ricostruzione archivi (polizza elettronica classica).

Conclusioni

Lo spazio di un focus-on permette solo di introdurre l'argomento stima dei danni e gestione del trasferimento del rischio. Il tema è di grande attualità e la gestione di molti aspetti è ancora oggetto di discussioni strategiche sia nel mondo assicurativo che nel mondo delle aziende.

Come al solito, un certo livello di rischio andrà accettato, o perché davvero accettabile o perché non si può fare diversamente. L'importante è conoscere il problema ed essere consci del come è stato gestito. Per non farsi sorprendere proprio nel momento peggiore, quello dell'emergenza.