WHITE PAPER COPERTURA CYBER RISK

Coordinamento:	Luca Moroni – Via Virtuosa Srls
Gruppo di Lavoro:	Cesare Burei, Debora Casalini – Margas Srl Ettore Guarnaccia – Banca Popolare di Vicenza Spa Marco Cozzi – Hypo Alpe Bank Spa Andrea Cobelli – Azienda Trasporti Verona Srl
Revisione:	Luigi Gregori – Cogito Web Srl

Classificazione:		Pubblico	
Riferimento		**WPCR2016**	
Versione	1.0	Ultima Revisione	05/12/16

Firma digitale

Questo documento è firmato digitalmente da Luca Moroni. Se nella copia che state consultando la firma non è presente il documento è stato modificato e non è autorizzato alla divulgazione.

Firmato da:
Gianluca Moroni
Motivo:
Firma White Paper

Luogo:
Schio (VI)
Data: 05/12/2016 10:37:17

Premessa

Visitando le aziende e gli uffici IT vengo spesso accompagnato in zone relegate degli uffici della direzione. A volte mi ritrovo a parlare con persone che sono consapevoli dei rischi e che sconsolati ripetono “Lo abbiamo detto alla direzione che c’è un problema” a cui la risposta è sempre la stessa “L’informatica è un costo”. Anche adesso che si parla di innovazione che passa per il digitale, Fabbrica 4.0, IoT, Cloud ecc…

Qualche anno fa sono anche rimasto colpito perché una imprenditrice di seconda generazione, quasi una nativa digitale, si rivolgeva allo Staff IT dicendo "i ragazzi" quasi fossero dei garzoni di bottega, anche se erano dei professionisti che avevano molti anni più di lei. Questo è un caso estremo ma è la realtà in alcune aziende del Nord Est. Poi se i server non vanno, manca la connettività, le bolle non si stampano o l’automazione in produzione si ferma sembra che l’IT sia l’unico responsabile del problema. **Nelle aziende italiane c’è una generale sottovalutazione del rischi Cyber che in altri paesi sono invece presi molto sul serio**. Solo con la recente onda mediatica degli incidenti informatici legati ai “ransomware”, pare essere cresciuta la necessità di come tutelarsi e garantire la continuità nell’accesso ai dati in forma digitale. Alcuni IT Manager “virtuosi” hanno colto questa occasione per sensibilizzare l’azienda sul problema e di conseguenza iniziare un percorso di cambio di paradigma.

Il primo passo necessario è capire la situazione e i rischi. Questo va fatto con un pieno coinvolgimento della direzione dell’azienda che deve essere resa consapevole dei rischi Cyber presenti. Ogni attività è ormai pesantemente sbilanciata nell’informatica e solo un miope può pensare che una azienda, anche piccola, possa riuscire a non compromettere il proprio business se fosse isolata da internet, se i computer e i server fossero bloccati e se non fosse in qualche modo prevista una strategia di ripristino da un disastro.

Tuttavia il rischio non è concentrato solo sul blocco del funzionamento. Basti pensare ad un danno reputazionale. Quanti di voi che sono abituati a leggere le recensioni on line andrebbero a mangiare in un ristorante che non avete mai provato e che fosse contrassegnato da una sola stellina?. Se leggete delle recensioni negative sul cibo o il servizio è difficile che ceniate in quel locale. Questa è la reputazione digitale, diversa da quella reale e aumentata da Internet. Un attacco mirato a compromettere la reputazione di una azienda non è diverso da un attacco che mira a compromettere i server. Entrambe influenzano il business.

Quel che mi sembra di poter dire è che oggi ci troviamo ancora attori di uno scenario in cui il reparto informatico è consapevole di alcuni rischi, mentre la Direzione è poco sensibile al fatto che questi possano pesantemente influenzare il business in generale. Una analisi sui fattori di rischio cyber fatta usando dei framework di riferimento come la norma 27001 (specifica sulla sicurezza delle informazioni) ci può aiutare a identificare e mettere in rilievo delle vulnerabilità che si dividono i due gruppi con un peso di 80-20. L’80% delle vulnerabilità richiede uno sforzo ridotto per mitigare i problemi (Patch mancanti, Password deboli…). Il 20% residuo si divide in 10% di criticità che richiedono un investimento e 10% di criticità che non giustificano investimenti poiché sarebbero troppo elevati a fronte della loro percentuale di probabilità di accadimento.

Questo documento si focalizza sul 10% denominato “Rischio Cyber Residuo” e vuole avvicinare la domanda con l’offerta cercando di dare una risposta a chi gestisce i sistemi IT e sa esattamente quali sono le criticità e un mondo di assicuratori che non comprende quali solo i reali rischi che coinvolgono l’IT e che il manager informatico non può coprire-ma può voler portare all’attenzione del board.

Ringrazio tutte le persona che si sono impegnate nella ricerca e nella stesura dei testi che hanno portato a questo documento.

Luca Moroni

Executive Summary

Le assicurazioni Cyber sono state create per coprire il rischio residuo che non può essere mitigato con delle opportune misure di sicurezza. Ipotizzo che se oggi esistesse una assicurazione legata alla compromissione Ransomware[1] e se il premio fosse ragionevole, le aziende potrebbero considerarla come investimento su indicazioni dell'ufficio IT.

Il mercato è frammentato ed è necessario mappare i rischi reali su adeguate coperture assicurative. L'adozione di opportune misure di sicurezza, a seguito di una analisi per identificare le criticità, copre circa l'80% / 90% dei rischi evidenziati. Una assicurazione cyber deve coprire un rischio residuo che opportunamente misurato può essere gestito. Verrà analizzato il reale stato di esposizione al rischio delle aziende dell'area del Nord Italia e di come una metodologia oggettiva dimostri quanto è necessario spostare fuori dall'azienda il rischio Cyber residuo.

Nelle pagine che seguono si cercherà di fare chiarezza su questo argomento per fornire delle indicazioni alle aziende che stanno valutando una polizza Cyber.

Destinatari

I destinatari di questo documento sono i CIO e che devono essere consapevoli e iniziare a ragionare come un Risk Manager. Adottando una metodologia oggettiva e ripetibile devono riuscire a misurare il rischio quantificando l'importanza degli asset. Il documento deve essere condiviso con la direzione aziendale in quanto unica responsabile per la gestione del rischio residuo cyber. La direzione o il Risk Manager dovranno poi effettuare la scelta sulla polizza più adatta.

I destinatari sono anche le compagnie assicurative che devono agevolare l'adozione di una politica di prevenzione che permetta di misurare un rischio proporzionale alle misure di sicurezza che una azienda ha adottato. Volgiamo anche presentare dei possibili casi reali a cui il responsabile dei sistemi informativi (CIO) vuole una risposta. Tutto questo per cercare di avvicinare la domanda all'offerta. E se possibile adattare l'offerta a quello che effettivamente serve.

Metodologia

Il presente white paper si basa su due distinte indagini: una sull'esposizione al rischio e una sul grado di sensibilità e adozione di coperture cyber nelle aziende del Nord-Est. Il campione per l'esposizione al rischio è stato di circa 68 aziende misurato nell'arco di tre anni. Mentre alla survey sulla consapevolezza hanno risposto 63 aziende diverse ma sempre nello stesso territorio. Alla luce dei risultati abbiamo chiesto a 3 responsabili IT di sottoporre 18 domande all'assicuratore Cyber per avere un chiarimento. Prima di questo ipotetico confronto il Broker specializzato in ambito Cyber, ha fatto una panoramica sullo stato dell'arte su questa tematica dal punto di vista delle proposte presenti sul mercato.

Donazione

Il presente White Paper è gratuito ma non copiabile e riproducibile come indicato nella prima pagina. Se ritenete che il contenuto sia stato interessante e utile vi chiediamo di fare una donazione libera a favore di Telefono Azzurro http://www.azzurro.it/it/sostienici/fai-una-donazione con causale "ViaVirtuosa" o su un contro PayPal che abbiamo creato paypal.me/ViaVirtuosa . Con i fondi donati faremo una donazione a Telefono Azzurro per aiutare le vittime del Cyberbullismo. Al momento della donazione manderemo un ringraziamento alle persone che avranno contribuito alla cifra che verrà inviata. Ti ringraziamo se vorrai contribuire.

[1] https://it.wikipedia.org/wiki/Ransomware

INDICE	Pagina

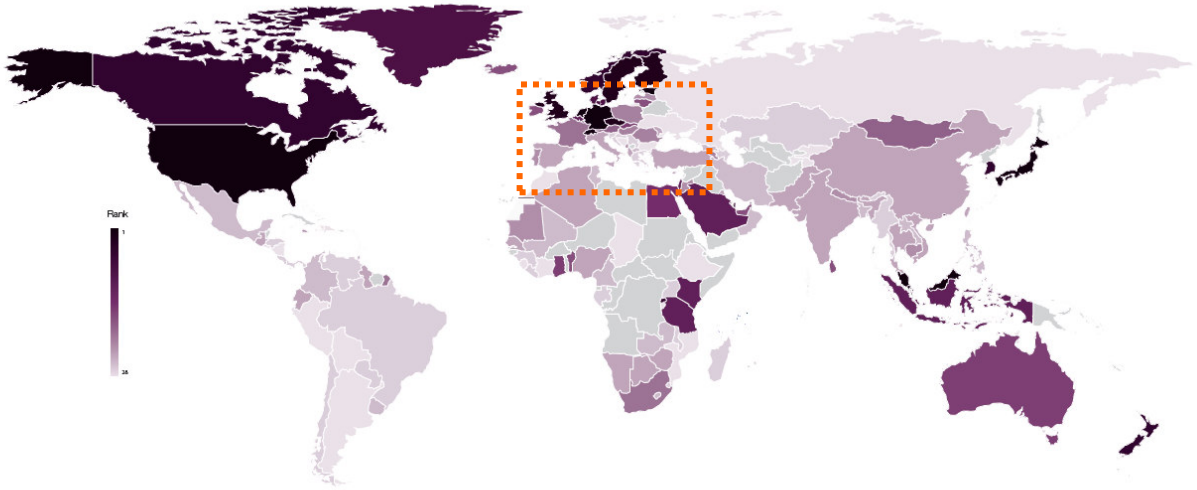
Cosa è il Rischio Cyber

Le definizioni attuali di Cyber Risk sono prevalentemente riconducibili a fornitori di prodotti assicurativi. ANIA - L'Associazione Nazionale fra le Imprese Assicuratrici – aveva stimato per il 2016 una decrescita di oltre il 7%[2] per le polizze tradizionali mentre si parla di un aumento del 300%[3] per le polizze Cyber. Proprio alla luce di una impennata del mercato si assiste ad una offerta esplosiva di prodotti assicurativi sulla sicurezza informatica. Concretamente tuttavia le Assicurazioni non dispongono di standard per la valutazione del rischio.

Partiamo dalla definizione, il Rischio Cyber può essere visto come "il rischio connesso all'uso delle tecnologie informatiche e di internet"[4]. La prima domanda è quale area di business in una azienda non sia basata sulle tecnologie?

Su questo aspetto assistiamo ad una accelerazione degli investimenti legati alla fabbrica 4.0[5], strada obbligata per il tessuto produttivo italiano fatto prevalentemente di aziende manifatturiere in lotta per la competitività globale, ma storicamente poco sensibili all'evoluzione informatica, mentre le maggiori aziende del mondo sono tecnologiche o guidate dalla tecnologia[6]. D'altra parte **Il World Economic Forum, nel suo report sui rischi globali del 2016[7] , pone attenzione al rischio della dipendenza tecnologica**. : L'interconnessione digitale delle persone, delle cose (IoT) e delle organizzazioni esporrà al rischio cyber il business di ogni azienda ed in particolare attraverso attacchi criminali. testimonia l'attenzione che deve essere posta al Rischio Cyber nel business di ogni azienda. Dalle analisi emerge che il rischio di Cyberattacco è uno fra i principali rischi a livello mondiale.

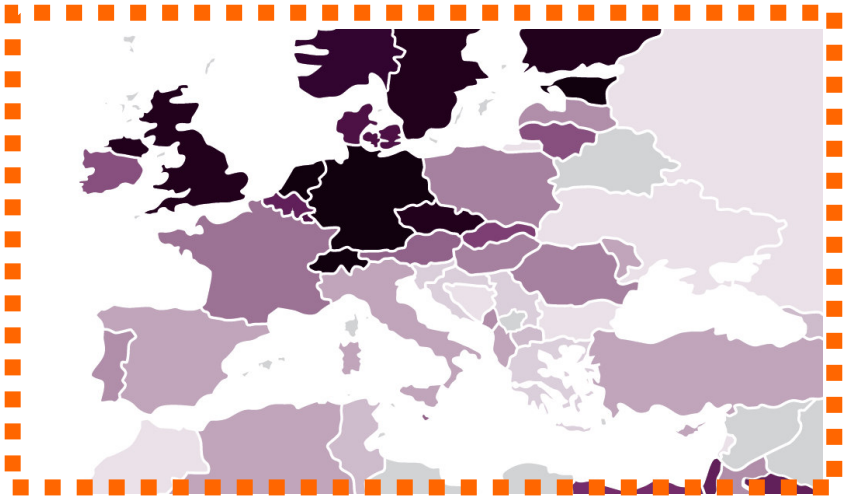
Figure 4.6 Cyberattacks, rank



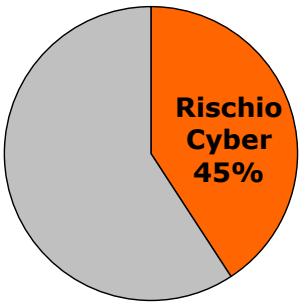
Source: Executive Opinion Survey 2015, World Economic Forum.
Note: The darker colour, the higher the concern.

[2] I dati significativi del mercato assicurativo italiano Presentazione del rapporto annuale L'ASSICURAZIONE ITALIANA 2015 - 2016 Sergio Desantis
[3] https://www.assinews.it/01/2016/boom-delle-cyber-assicurazioni-le-sfide-del-settore/550034489/
[4] https://techcrunch.com/2016/06/13/cyber-insurance-is-changing-the-way-we-look-at-risk/
[5] https://www.key4biz.it/industria-4-0-cina-e-germania-investono-litalia-che-fa/139792/
[6] https://www.key4biz.it/internet-of-things-lindustria-manifatturiera-mondiale-investira-70-miliardi-entro-il-2020/152203
[7] The Global Risks Report 2016 11th Edition by the World Economic Forum

Vediamo anche uno zoom sull'Italia e sui paesi a noi vicini



Il Report di Cyber Security National Lab[8] a Ottobre 2015 riporta ~~questo testo~~ "***Il miglioramento delle difese del cyberspace sarà pertanto uno dei requisiti che guiderà gli investimenti da parte di operatori internazionali, i quali non sono interessati ad insediamenti industriali in assenza di un'adeguata organizzazione e capacità difensiva cyber***". Questo per evidenziare quanto il rischio Cyber e la sicurezza dei dati diventano un valore di business. L'Allianz Risk Barometer 2016[9] valuta che per i Risk Manager intervistati (circa 800) la **Business Interruption** è il rischio più temuto. Questo è influenzato pesantemente dalle tecnologie. Ma al terzo posto si posiziona **l'incidente Cyber**. Sempre influenzati dalle tecnologie sono la **perdita di reputazione** al settimo posto, fino al decimo posto con i **furti e le frodi**. Sintetizzando questi quattro rischi e riconducendoli alle tecnologie arriviamo ad un valore di circa il 45%.



Totale rischi sul business 100%.

Una crescete attenzione al livello di sicurezza delle informazioni in Germania sta avendo riflessi anche sulla percezione del problema da parte delle aziende italiane che fanno parte di Konzern tedeschi o intrattengono forti

[8] http://www.ilsole24ore.com/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Correlati/Documenti/Notizie/2015/11/CyberSecurity-Report.pdf
[9] http://instoremag.it/featured/la-top-10-dei-rischi-piu-temuti-dalle-aziende-in-testa-ancora-la-business-interruption/20160119.81097

relazioni commerciali con questo paese. Il governo ha imposto una attenzione particolare[10] imponendo per legge la certificazione entro il 2017 secondo la norma 27001 della aziende critiche più importati: Questo ha poi avuto un riflesso su tutte le maggiori aziende tedesche. Anche gli USA con il Cybersecurity National Action Plan hanno dato un impulso pesante alla Cybersecurity. Per cui oggi avere un livello di maturità nella gestione della sicurezza delle informazioni diventa un asset di valore. Secondo il recente report di Ernst&Young declinato per l'italia il 71% degli responsabili della Cybersecurity in azienda valuta come necessario l'aumento del Budget da destinare alla Cybersecurity, anche se meno del 50% ammette che gli investimenti rimarranno costanti nei prossimi mesi.[11]

Misurare il rischio Cyber

Tipico vettore del Ransomware malware è il Phishing[12] e non esiste ad oggi uno strumento consolidato di rilevazione preventiva. Per cui il bastione nelle aziende è lasciato alla consapevolezza dei dipendenti, che in genere è molto bassa. Ma quanto bassa? Riusciamo a misurarla? Le attività di ingegneria sociale volte a rispondere a quelle malevole e cioè anche a misurare la consapevolezza del rischio delle persone egli errori che commettono nelle organizzazioni è molto recente. Ma già uno sguardo al comportamento sui social network dove cliccare, ritwittare, commentare notizie palesemente fasulle da siti improbabili è la norma, non l'eccezione, ci può far dedurre che sia un aspetto fuori controllo anche nelle aziende.

Secondo la ricerca[13] di ENISA che è l'Ente Europeo della Sicurezza Informatica, questa è la tipologia di incidenti cyber che hanno creato una perdita.

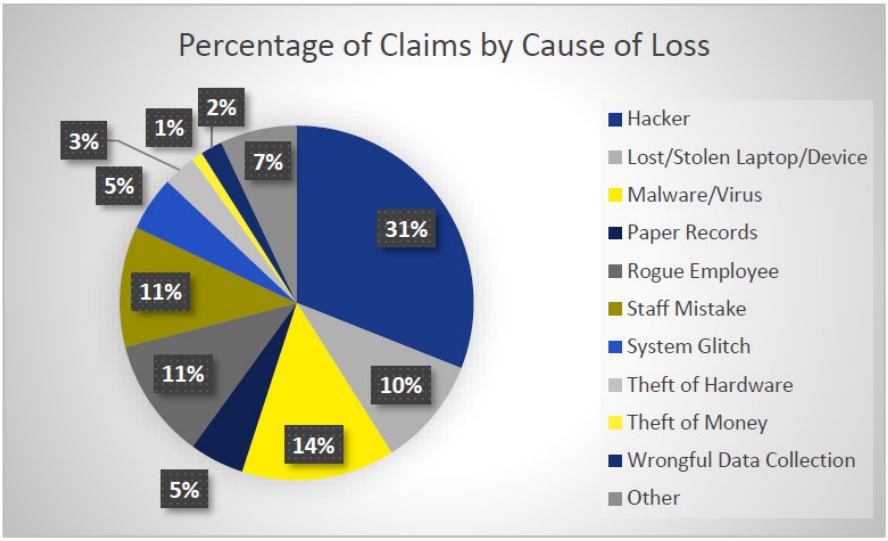


Figure 3: Claims by Cause of Loss (2012 – 2015)[25]

Non è prioritario far comprendere all'IT Manager quali sono i maggiori rischi IT sopra identificati. **Forse l'IT Manager va aiutato a vedere il problema in modo più completo in una logica di misura**. L'IT manager deve essere informato e conoscere il livello di rischio, se non c'è un Risk Manager in azienda. Deve poter misurare il rischio in modo oggettivo e ripetibile. Deve documentare la situazione e adottare una strategia di mitigazione. Questo va fatto prima di valutare una assicurazione Cyber. Solo in questo modo potrà tradurre ai livelli apicali della sua azienda

[10] http://www.itgovernance.eu/blog/new-german-cyber-security-law-to-protect-critical-infrastructure/
[11] http://www.corrierecomunicazioni.it/digital/38497_cybersecurity-in-italia-investimenti-al-palo.htm
[12] https://it.wikipedia.org/wiki/Phishing
[13] Cyber Insurance: Recent Advances, Good Practices and Challenges – ENISA November 2016

l'urgenza nell'adottare una strategia di prevenzione sulla sicurezza informatica. Questa missione dell'IT Manager nel creare consapevolezza aziendale sembra molto difficile. Secondo una indagine del Politecnico di Milano[14] si afferma che **non esiste una vera e propria pianificazione alla resilienza ma una reazione solo in caso di incidente informatico**.

Creare una misurazione condivisa fra Assicuratore e IT Manager

Partiamo dalla esigenza di misurare la situazione usando un protocollo condiviso fra Assicuratore e IT Manager.
Questo è un esempio di tabella sinottica che analizza tutte le componenti che possono influenzare la sicurezza informatica. Tipicamente in una analisi viene misurato per ogni ambito la situazione di fatto e la complessità delle azioni necessarie per mitigare il rischio.

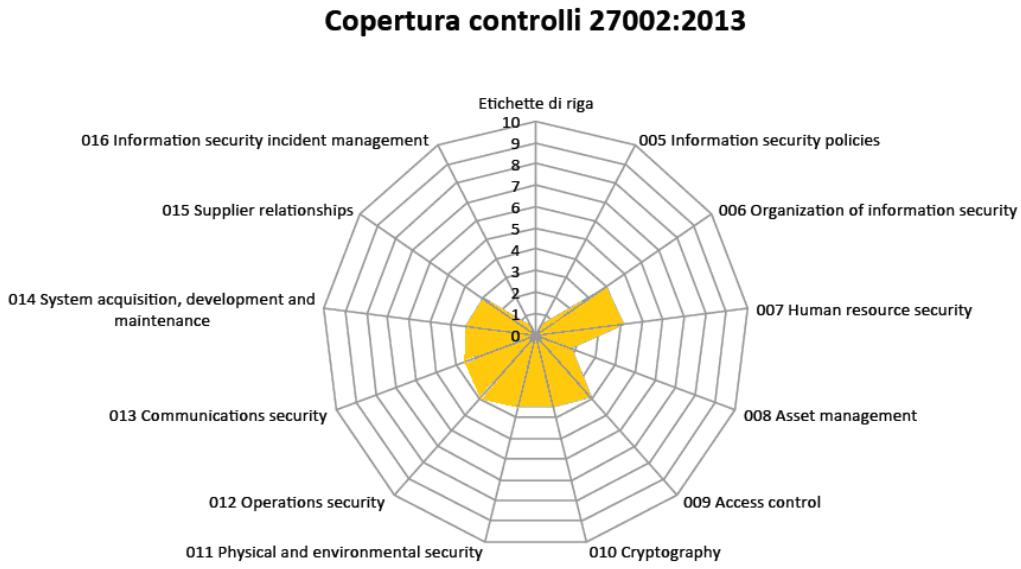
2.1 - Tabella sinottica

Descrizione	Stato di fatto	Azioni suggerite
Backup [continuità operativa, sicurezza]	Buono	Poco complesse
Disaster recovery [continuità operativa]	Buono	Nessuna
Aderenza alle leggi [normativa]	Buono	Poco complesse
Firewall [sicurezza, continuità operativa]	Buono	Poco complesse
Sicurezza fisica CED [sicurezza, continuità operativa]	Buono	Nessuna
Wireless [sicurezza]	Rischioso	Media complessità
Comunicazioni di rete [sicurezza]	Rischioso	Media complessità
Dispositivi portatili (laptop, tablet, smartphone) [sicurezza]	Rischioso	Media complessità
Segmentazione rete [sicurezza]	Rischioso	Complesse
Credenziali [sicurezza, normativa]	Migliorabile	Poco complesse
Postazioni di lavoro [sicurezza, gestione]	Migliorabile	Media complessità
Aggiornamenti di sicurezza [sicurezza]	Migliorabile	Poco complesse
Apparati di rete principali [continuità operativa]	Migliorabile	Poco complesse
Gestione sistemistica [sicurezza, gestione, continuità operativa]	Migliorabile	Media complessità
Monitoraggio [continuità operativa, gestione, sicurezza]	Migliorabile	Poco complesse
Dismissione hardware e apparati [sicurezza]	Migliorabile	Poco complesse

Come si vede gli ambiti sono di tipo IT ma anche Organizzativi, Legali. Il rischio di sicurezza informatica aziendale è fatto di diverse componenti ma il rischio Cyber è prevalentemente legato all'IT anche se darne un valore economico Ex Ante è molto complesso. Mentre Ex Post, ad incidente avvenuto spesso ci si rende conto che una strategia di mitigazione avrebbe avuto un costo molto più basso. La mancanza di un campione esteso di incidenti e di danni economici conseguenti, sono oggi uno dei problemi per gli assicuratori per il calcolo del rischio.

Riportiamo il diagramma a Radar sulla norma 2700x (che può considerarsi standard di riferimento riconosciuto a livello internazionale) per capire gli ambiti aziendali che vanno analizzati per misurare oggettivamente la situazione. Esistono molti standard e declinazioni specifiche per i settori di business o le aree aziendali. Uno standard generale che abbia un riconoscimento internazionale, permette ad una azienda Italiana di fornire dei dati ad una compagnia assicurativa estera.

[14] https://www.digital4.biz/searchsecurity/compliance-governance/polimi-il-42-dei-budget-italiani-allocato-alla-voce-information-security--privacy_43672157185.htm



Lo Standard ISO/IEC 27001:2013 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) è una norma internazionale oggettiva che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.[15] Questo standard sta diventando il framework di riferimento e molte aziende misurano la propria maturità valutando la distanza da i requisiti necessari ad ottenere una certificazione.

L'adozione di un Framework come la 2700x per una PMI è forse troppo complesso e forse non esaustivo, ma **potrebbe costituire uno standard di base comune fra IT Manager e Assicuratore**. Un primo approccio potrebbe essere una auto valutazione (domande a cui rispondere) basato su questa norma o meglio una Analisi di distanza 2700x fatto da una terza parte qualificata.

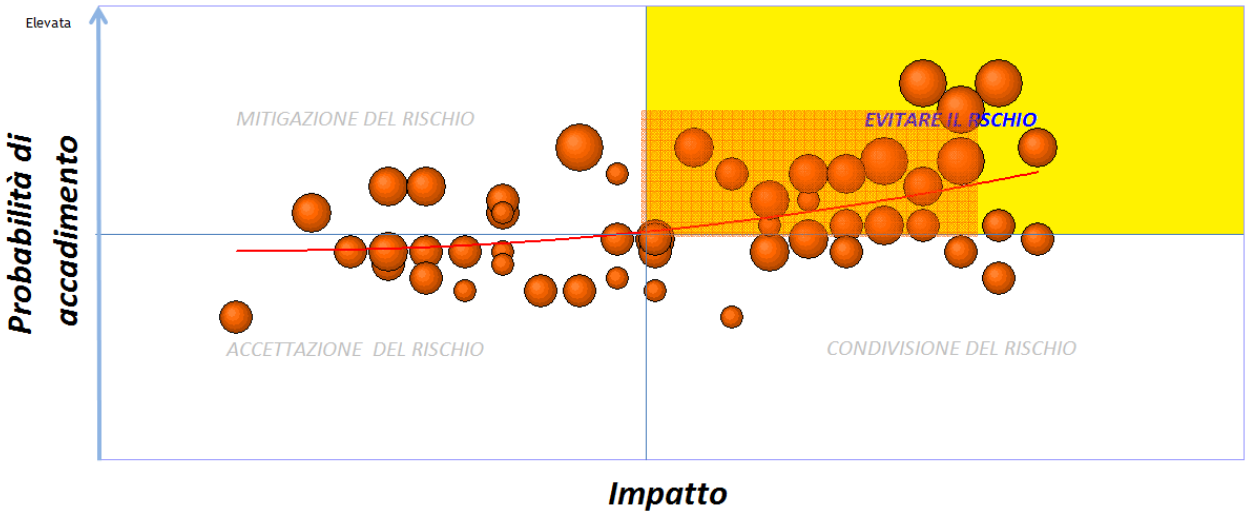
Cerchiamo di capire quanto il rischio Cyber può essere importante all'interno della azienda.

Un analisi di esposizione al Rischio Cyber sulle aziende del Nord Italia

Analizzando un campione di circa 68 aziende del Nord Est che hanno risposto ad un questionario basato sulla metodologia dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) "Determining Your Organization's Information Risk Assessment and Management"[16] è emerso che circa un 30% sono posizionate in un'area di Rischio del diagramma (zona gialla). L'importanza dello studio è dato da una metodologia di misurazione oggettiva e ripetibile in relazione ad un certo territorio. Il diagramma di sintesi evidenzia che questo 30% sono aziende di medio/grandi dimensioni (*dimensione della sfera*) secondo la classificazione seguente:

- Aziende medio grandi, con un certo numero di collaboratori, sedi in più di un paese
- Multinazionali con molti collaboratori (e sedi dislocate in molti paesi)

[15] https://it.wikipedia.org/wiki/ISO/IEC_27001
[16] https://www.enisa.europa.eu/publications/archive/determining-your-organization2019s-information-risk-assessment-and-management



La ricerca svolta da Via Virtuosa nell'arco di 3 anni, evidenzia non tanto il posizionamento della singola azienda e la sua 'esposizione al rischio, bensì l'andamento statistico di un certo territorio nello specifico quello del Nord Est italiano (campione intervistato) e una Base Line di riferimento (Linea Rossa) con cui potersi confrontare. La metodologia di misurazione è oggettiva (come per la 2700x) per cui uguale per tutto il campione anche se notevolmente più basilare. **Poter avere una misurazione oggettiva del rischio cyber, permetterebbe di sottoporre una richiesta di pari polizza a più compagnie**.

Chi rientra nel quadrante in alto a destra (giallo) ha una esposizione al rischio significativa e con un impatto significativo sul business in caso di incidente. Chi si trova in questo quadrante viene invitato (secondo la metodologia di un Ente Europeo focalizzato sulla sicurezza informatica) ad ESTERNALIZZARE IL RISCHIO.

Questa ricerca ha fatto emergere questi aspetti:

- Elevato rischio Cyber per le aziende e forte esposizione al rischio di business essendo sbilanciate nell'uso della tecnologia.
- Consapevolezza del reparto IT sul problema ma mancanza pressoché totale di sensibilità sul problema da parte del board aziendale. Per cui scarsi investimenti.
- Mancanza di una misurazione oggettiva del rischio Cyber da parte delle aziende.
- Investimenti in crescita e consapevolezza in molti paesi europei legato ad una definizione di rischio elevato identificato da aree di business non IT.
- Indicazioni oggettive di spostare il rischio Cyber all'esterno dell'azienda.

Questa metodologia o l'utilizzo di una analisi secondo la norma ISO potrebbero costituire un protocollo di intesa fra il Responsabile IT e l'Assicuratore. Quest'ultimo analizzando i risultati dell'analisi e la mitigazione attuata dall'azienda potrebbe avere un quadro oggettivo su cui proporre una copertura del rischio residuo.

Lo scenario dal punto di vista dell'Assicuratore

C'è chi è già stato *hackerato* dall'esterno o ha avuto un problema cyber-correlato interno. C'è chi si confronterà con questi temi in futuro. La terza opzione "a me non succederà" è assai improbabile vista la pervasività della dimensione digitale e il fatto che l'operatività delle nostre aziende è fortemente fondata sul web, sui device mobili o sull'attività umana in questi ambiti. Anche a causa dell'assenza o della limitatezza, almeno per ora, di norme stringenti e cogenti in materia, pochi parlano apertamente delle loro esperienze rallentando non poco il percorso di crescita di consapevolezza e informazione del sistema "Aziende"o l'adeguatezza dell'offerta assicurativa, in particolare in Italia.
In questo contesto la polizza assicurativa viene percepita più come un "di cui" dall'efficacia incerta che come un efficace e necessario strumento di trasferimento del rischio residuo e paracadute finanziario in grado di supportare le imprese nella loro sopravvivenza, reattività e competitività in caso di sinistro.
In assenza di un approccio diffuso di risk management nelle aziende italiane, specialmente PMI, o di Risk Manager skillati sulla comprensione degli aspetti informatici nelle realtà più strutturate e grandi, questa survey è stata indirizzata ai CIO che normalmente non si occupano di temi assicurativi, ma hanno la percezione del rischio diretto e indiretto, sono essenziali per la compilazione degli inevitabili questionari assicurativi ed hanno necessità di contrattare in azienda il loro budget per la sicurezza. Il CIO può dunque essere il motore della riflessione interna sullo stato dell'arte e contribuire a far nascere un tavolo di gestione condiviso.

Cyber Sinistro, ma quanto mi costi? Ecco perché la Cyber Insurance
Riprendiamo qui alcuni esempi tratti dal Clusit Report 2016 – Focus On Cyber Insurance.
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.

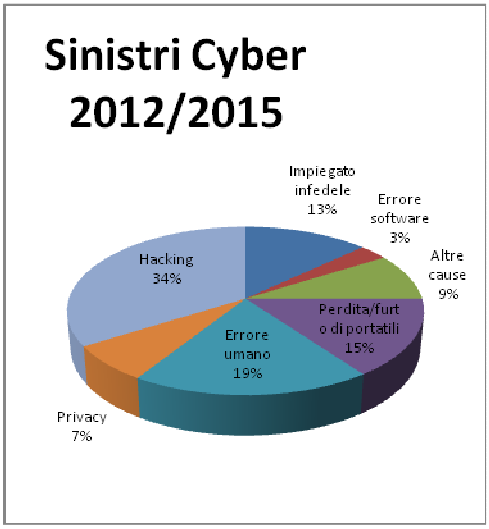
- Infezione da Virus nel settore: GDO; Tempo di ripristino: 10 giorni; costi straordinari (solo rete UE): 0,5 Milioni e; perdite di profitto risarcite: 0,6 Milioni e; perdita di mercato stimata massimo 7%
- Errori dello staff IT Settore: TLC; Tempo di ripristino: 85 giorni (migliaia di server della Rete); costi straordinari: 1 Milione e; perdite di profitto: non risarcibili perché escluse (stimate 55 milioni e).
- 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 e); perdite di profitto (stimate 2 milioni e), 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 e; perdite di profitto su rete 5.000 negozi (25.000 macchine): 14 Milioni e, risarciti 5 Me per sottoassicurazione.

- Logic Bomb nel sistema principale nel settore: Finanziario/Assicurativo; Tempo di ripristino: 88 giorni parziale; riparazione SW 54.000e; perdita da frode informatica (distrazione fondi): 10 milionie, 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 e (distrazione traffico telefonico), risarcimento 50.000 e 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).[17]

La Cyber Insurance in Italia

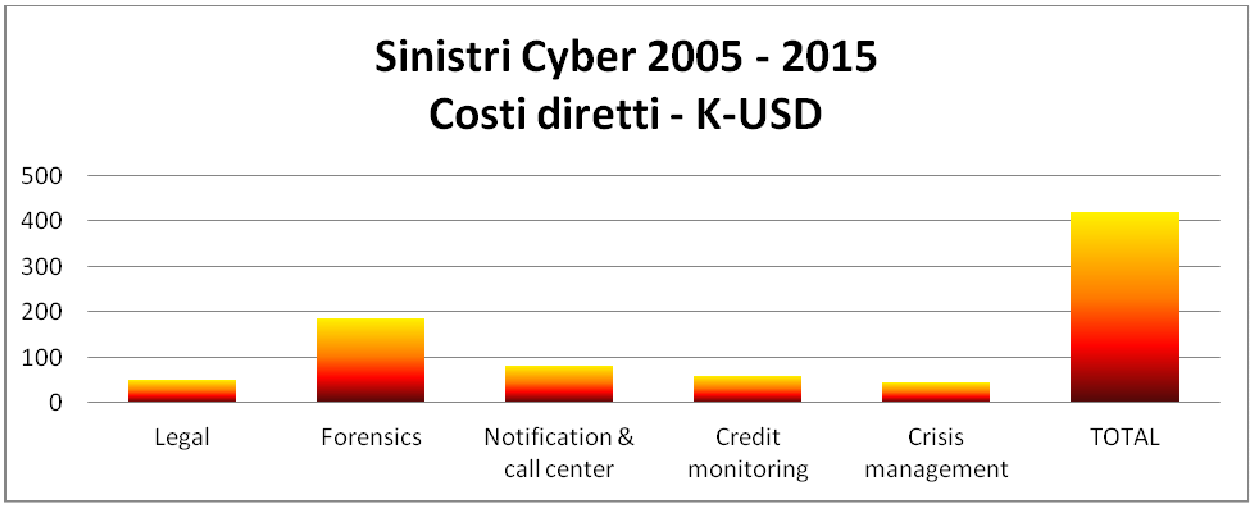
A fronte di una **domanda di Cyber Insurance** in rapida crescita ma recente, in Italia è piuttosto difficile trovare player specializzati, ma soprattutto in grado di valutare correttamente rischio e copertura assicurativa da proporre.
Il panorama italiano dell'offerta è presidiato essenzialmente da **CHUBB (Ex ACE Europe), Generali, AIG, Allianz AGCS, Unipol, Zurich, XLCatlin ed alcuni sindacati dei Lloyd's** con prodotti assicurativi abbastanza evoluti per far fronte ad un utenza business. Esistono anche altre soluzioni, come quelle proposte da **Dual** o da **AXA**, specificatamente tarate su target medio/piccoli.
Data la scarsa diffusione dei contratti assicurativi Cyber, i dati più rappresentativi sullo status quo del mercato assicurativo, sull'entità dei sinistri e loro tipologia provengono essenzialmente dal mercato americano, dove da anni vige l'obbligo di notifica da parte delle imprese quando colpite da incidenti di tipo cyber.

Qui di fianco riportiamo i dati aggregati delle tipologie di sinistro denunciate negli ultimi tre anni diffuse recentemente da Chubb[18]. Spicca la componente dell'errore umano e della perdita/furto di laptop, componenti endogene all'attività aziendale e che insieme equivalgono all'impatto dell'hacking proveniente dall'esterno.



Interessante anche il dato sull'impatto medio di un sinistro cyber, dovuto a causa interna o esterna, riportato qui sopra in migliaia di dollari. Si noti che nella valutazione non rientrano i danni da *businness interruption*, che spesso superano di un ordine di grandezza i costi diretti e le cui conseguenze si possono prolungare per diversi mesi dopo il sinistro.

[17] Rapporto Clusit 2016 sulla Sicurezza ICT in Italia – Focus ON: Assicurare il rischio Informatico – AA: Chubb, Margas, Obiectivo
[18] Fonte: Chubb Claim Trends 8/2016



Fonte: Chubb Claim Trends 8/2016

Alla luce di quanto sopra, possiamo confermare che negli USA il mercato assicurativo cresce costantemente di un 30% annuo con premi incassati nel 2015 per 1,3 Mld di Dollari, pari a circa il 90% del mercato mondiale.
In Europa il potenziale di crescita è considerato elevato. L'aumento dei rischi e il progressivo giro di vite da parte di organi di controllo fa prevedere per i prossimi due anni una crescita annua del 50%. Secondo stime di Allianz AGCS entro il 2018 dovremmo raggiungere un volume di premi tra i 700 e i 900 Mln di Euro, a fronte comunque di un potenziale impatto da sinistro cyber pari a qualche miliardo di Euro[19].
Parte della responsabilità di questo ritardo, oltre che in una legislazione non cogente, sta anche nel ritardo con cui intermediari e broker assicurativi hanno cominciato ad inserire il tema Cyber-Risk in quello che dovrebbe essere un aspetto importante del rapporto col cliente, ovvero l'intervista periodica sull'aggiornamento dei rischi aziendali.

Che cosa è e come si presenta una polizza cyber.
Il processo valutativo e di selezione

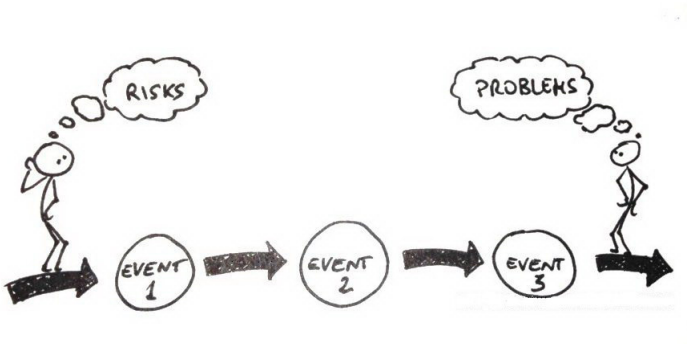
E ' bene ribadire che una polizza cyber deve essere considerata come un supporto tecnico-finanziario **volto a proteggere il business da rischi connessi con infrastrutture e attività ICT e internet based.** Se correttamente strutturata, compensa i costi e danni incerti e imprevisti a fronte di un costo finanziario certo, valutabile in anticipo su base annua.
Molto importante è ricordare anche che in taluni casi il cyber risk può essere correttamente integrato nelle **coperture assicurative tradizionali** e deve essere comunque affiancato costantemente **da alcune buone pratiche** che, in maniera molto schematica, possiamo riassumere in:

- apertura di un tavolo aziendale sul Cyber Risk a cui partecipino tutti i soggetti apicali interessati, con follow-up periodici su miglioramenti e nuove problematiche;
- formalizzazione di un regolamento per l'utilizzo dell'infrastruttura informatica;

[19] Wolters Kluwer Deutschland: http://www.gvnw.de/fileadmin/user_upload/Publikationen/Wolters_Kluwer_Cyber-Versicherung_Leseprobe.pdf

- formazione del personale interno;
- simulazione di situazioni critiche e scenari di intervento, con valutazione dei tempi di reazione anche nei confronti del comportamento umano;
- bilancio periodico tra interventi in Cyber Risk Management e potenziali perdite.

Il processo sopra descritto è importante non solo per difenderci da "minacce informatiche" esterne e in continua mutazione per le quali si comincia ad investire in tecnologie, ma anche da quelle endogene all'attività aziendale di cui ci si preoccupa meno, ma che pesano ugualmente. Quindi, seppur ben difesi dall'esterno, siamo molto esposti se il processo di Risk Management interno non è completo e continuo.
Inoltre questa attività è fondamentale per definire il rischio residuo nel suo perimetro tecnico e finanziario e dunque per porre correttamente all'assicuratore le nostre esigenze.



Le **polizze tradizionali** con cui mettere in relazione la copertura cyber o da analizzare in ottica cyber prima di prendere delle decisioni sono:

- Polizza Incendio
- Polizza Danni Indiretti o Business Interruption
- Polizza Elettronica
- RC Generale – Responsabilità Civile Generale
- RC Professionale – Responsabilità Civile Professionale
- RC Prodotti – Responsabilità Civile per prodotto difettoso
- D&O – Responsabilità degli Amministratori e dei Dirigenti

Dalla lettura dei testi emerge che le polizze spesso non considerano, o peggio, escludono in maniera specifica problematiche ICT correlate.
Una copertura cyber è di solito strutturata in **macro-moduli attivabili o meno,** generalmente riguardanti:

- Responsabilità Civile verso Terzi, tipicamente per violazione della privacy o utilizzo non autorizzato della infrastruttura informatica;
- Costi di reazione indennizzabili a fronte di sinistro;
- Danni indiretti.

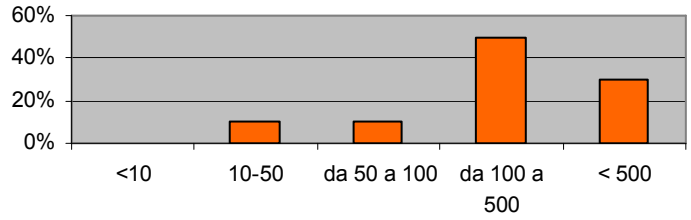
Chi si approccia all'attività di analisi assicurativa si troverà anche a leggere **definizioni di polizza**, fondamentali per definire i *trigger* di attivazione del contratto, diverse a seconda del testo oggetto di lettura. Per capire quindi **cosa è effettivamente trasferibile all'assicurazione ed il perimetro di copertura,** senza voler scendere nel dettaglio di una analisi comparata, vi rimandiamo al capitolo successivo, dedicato a rispondere a **domande specifiche poste dai CIO**

coinvolti nella stesura del presente white paper e molto rappresentative di quelle che vengono costantemente rivolte a chiunque si trovi ad operare nel settore assicurativo e in particolare nell'ambito Cyber Insurance.

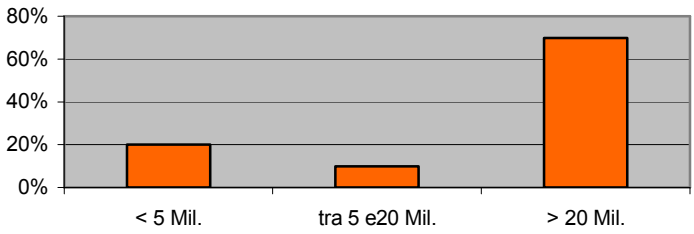
SURVEY sul livello di sensibilità al rischio cyber e al suo trasferimento assicurativo

Abbiamo predisposto un sondaggio costituto da 12 domande di cui le prime 3 per qualificare il campione. Nel periodo dal 13 maggio 2016 fino al 3 Luglio 2016 hanno risposto 63 aziende posizionate nel Nord Italia. I destinatari erano preferibilmente CIO e Risk Manager. Le domande specifiche sono state definite dall'Assicuratore per comprendere il livello di competenza sulla materia del CIO e lo scenario esistente.

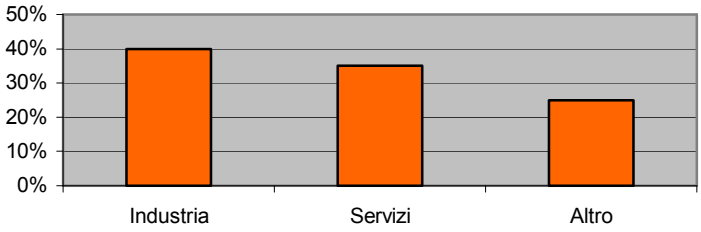
FASCIA DIPENDENTI



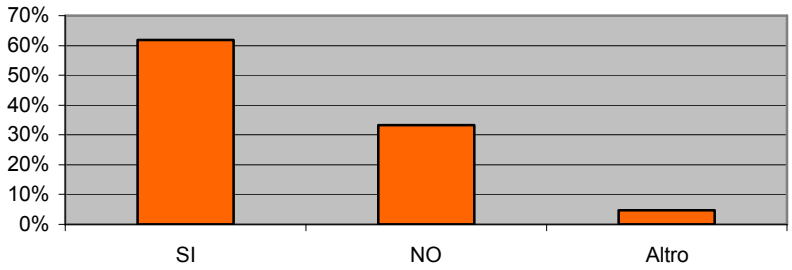
FASCIA FATTURATO



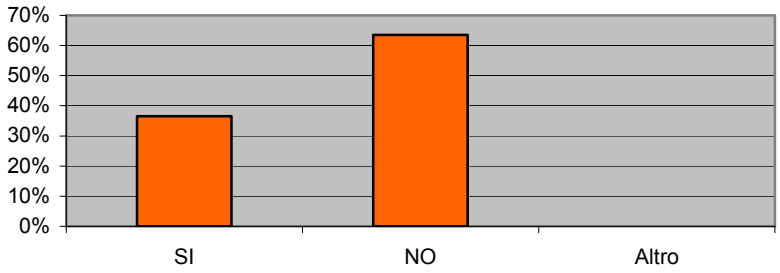
SETTORE



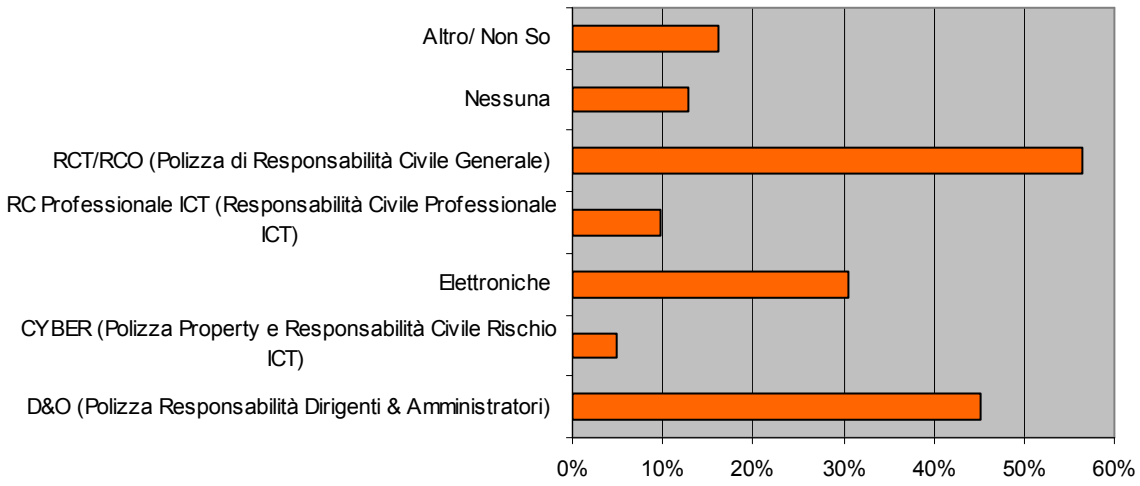
DOMANDA 1: Come responsabile ICT è mai stato coinvolto in tavoli di gestione della sicurezza generale aziendale?



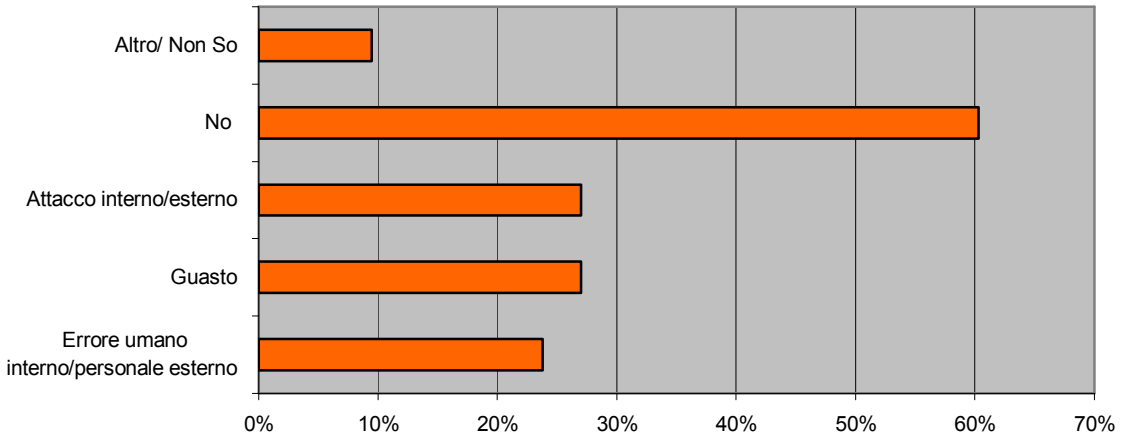
DOMANDA 2: Ha mai chiesto di conoscere le esclusioni/coperture delle polizze assicurative esistenti?



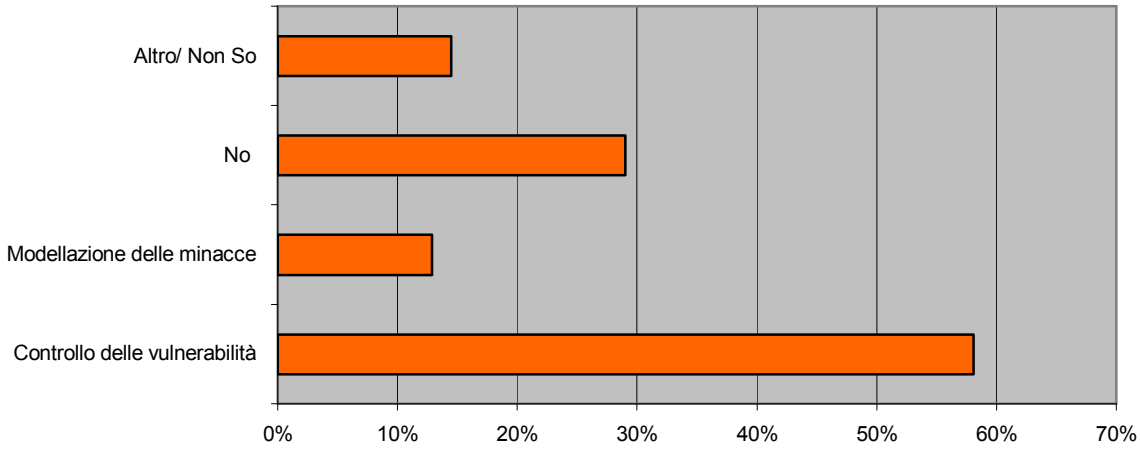
DOMANDA 3: Esistono in azienda queste polizze? (Anche più di una risposta)



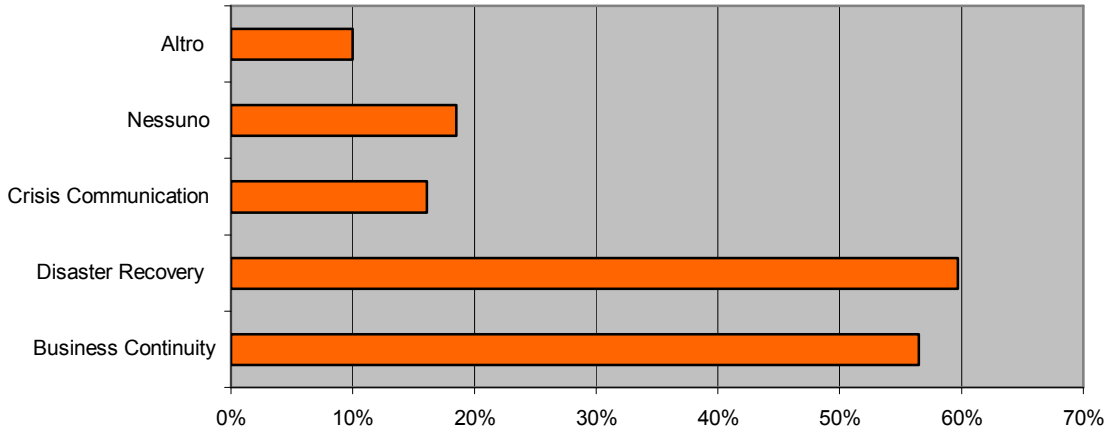
DOMANDA 4: Le hanno mai chiesto di evidenziare i costi/danni che presume possano derivare da un sinistro cyber? (Anche più di una risposta)



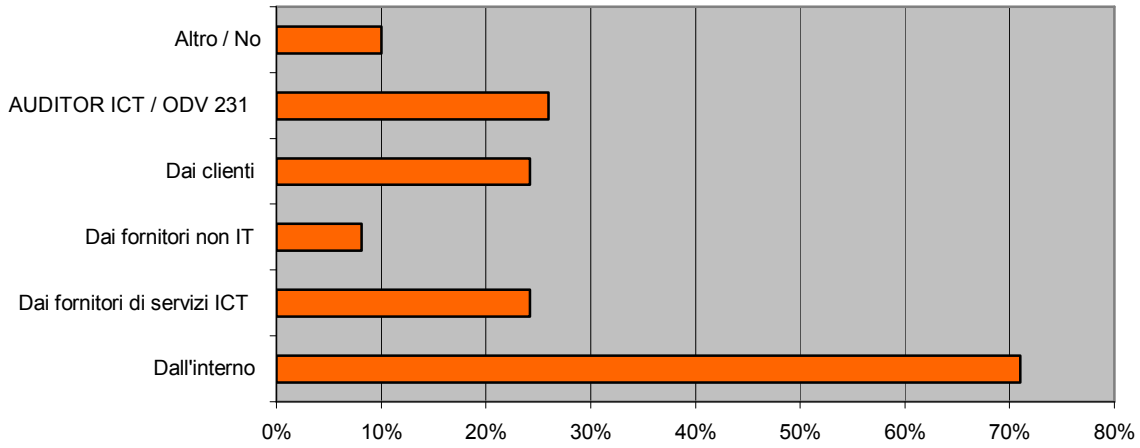
DOMANDA 5: Sono formalizzate politiche/procedure di sicurezza ICT? (Anche più di una risposta)



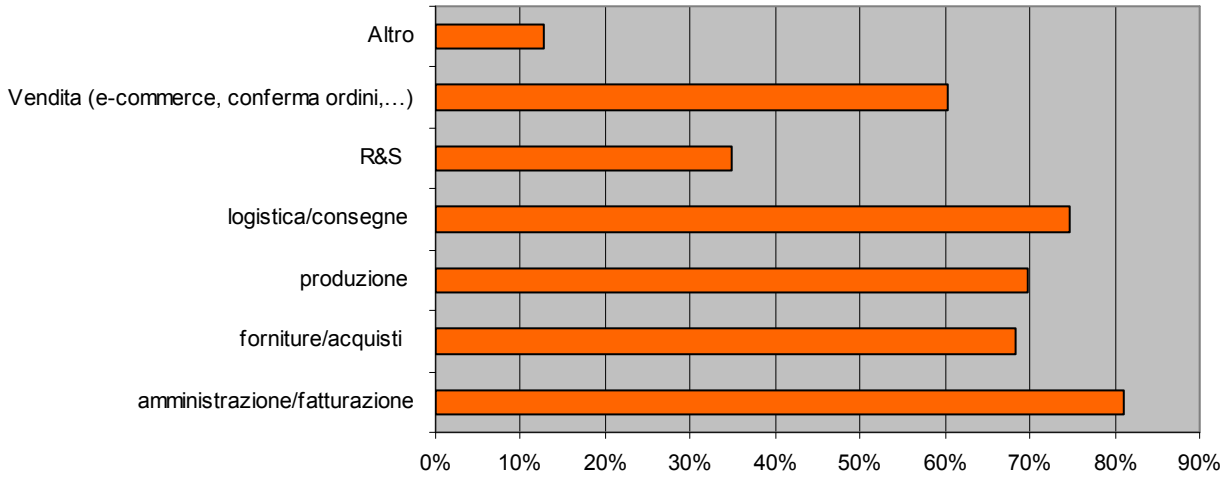
DOMANDA 6: Esistono piani di: (Anche più di una risposta)



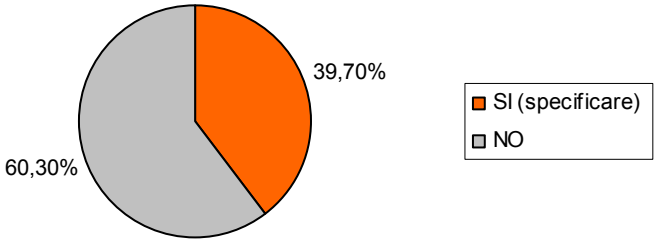
DOMANDA 7: All'ICT manager sono pervenute richieste in merito alla gestione della sicurezza ICT? (Anche più di una risposta)



DOMANDA 8: Un fermo di attività ICT su quali aree di lavoro aziendale può impattare (Anche più di una risposta)



DOMANDA 9: Sa dire se ci sono stati negli ultimi 5 anni sinistri cyber o analogici con impatto ICT e come sono stati gestiti?



NOTE: La maggior parte dovuti a Ransomware.

Il punto di vista del CIO – Tre business Case

Abbiamo chiesto a 3 responsabili che in azienda seguono la sicurezza logica di fare alcune considerazioni sull'esito del survey presentato sopra. Abbiamo poi chiesto di illustrare il loro punto di vista sulle polizze cyber. Infine abbiamo chiesto di formulare alcune domande al Broker sulle polizze per avere una risposta con qualche indicazione utile. Le risposte sono sintetizzate nel capitolo successivo con le risposte.

1) Dr. Ettore Guarnaccia - Responsabile ICT e Sicurezza Logica del Gruppo Banca Popolare di Vicenza

In un mercato nazionale in cui il concetto di rischio è generalmente poco compreso, parlare di rischio *cyber* può talvolta sembrare pura fantascienza. Fortunatamente, il settore bancario italiano vanta sul tema un livello generale di maturità sensibilmente più avanzato rispetto agli altri settori nazionali, sebbene debba comunque scontare un certo *gap* con il livello di maturità di altre nazioni occidentali, con particolare riguardo al mondo anglosassone.
In moltissime banche italiane è oggi piuttosto comune parlare di gestione del rischio, una pratica ormai consolidata nel *framework* dei controlli interni, grazie anche al forte impulso generato dal crescente volume di disposizioni in materia di vigilanza bancaria. Un po' meno comune è il tema della gestione del rischio informatico – disciplina che include di fatto il rischio *cyber* – poiché le normative che ne hanno reso obbligatoria l'attuazione sono relativamente recente e molti istituti e gruppi bancari sono tuttora impegnati nell'allestimento di competenze, metodologie e processi a riguardo.
La spinta normativa ha certamente generato un aumento del livello di competenza e consapevolezza degli IT manager bancari, ma è condivisibile che essi vadano comunque aiutati a considerare il problema della gestione del rischio in modo più olistico. Ciò è dovuto all'ancora troppo elevata lontananza dell'IT dal *top management* aziendale, al differente linguaggio adottato dai due mondi – *business e information technology* – e alla carenza di punti di raccordo che mettano in comunicazione le due differenti culture. Da qui la diffusa frustrazione degli IT manager citata nel *white paper*.
Il rischio *cyber* è tipicamente originato dalla tecnologia, pertanto è generalmente – ed erroneamente – attribuito all'IT, ma i suoi potenziali impatti riguardano quasi sempre il business.
Il problema principale è tradurre un rischio di origine prettamente tecnologica in qualcosa di comprensibile al CEO e al CFO, in particolare per tutti quegli aspetti intangibili che vengono spesso trascurati e che invece vanno accuratamente stimati e quantificati. Mi riferisco, ad esempio, al danno reputazionale per l'immagine aziendale sul mercato che, in un mondo ipertecnologico e iperconnesso, può generarsi e diffondersi con pervasività e rapidità inarrestabili, mantenendo i propri effetti per lunghissimo tempo in virtù dell'incapacità del Web 2.0 di "dimenticare".
Ferma restando la necessità di un migliore allineamento fra business e IT, in materia di gestione del rischio informatico il raccordo più efficace fra l'alta direzione aziendale e il CIO (o il CISO) non può che essere costituito dal *risk manager* o, meglio, dall'*IT risk manager*. Il processo di gestione del rischio informatico, infatti, è attualmente l'unico processo che preveda il calcolo dei rischi connessi all'uso della tecnologia e la loro quantificazione in termini economici che siano comprensibili a chi si occupa del business aziendale.
Il risk manager ha il compito di effettuare l'analisi dei rischi informatici, collaborando con le funzioni IT e di sicurezza delle informazioni, per poi effettuarne la quantificazione economica in accordo con i rispettivi *owner* del business. In sede di approvazione dei rischi, il CEO, il CFO e il Consiglio di Amministrazione ottengono così una chiara e

comprensibile rappresentazione dei rischi derivanti dall'uso della tecnologia, ovviamente espressi in termini monetari, potendo così indirizzare al meglio gli interventi e gli investimenti per il loro trattamento.
Dato che siamo in tema di assicurazione del rischio *cyber*, va ricordato che fra le opzioni di trattamento dei rischi, oltre ad accettazione, mitigazione ed elusione, c'è il trasferimento, che nella maggior parte dei casi assume due particolari forme: l'esternalizzazione e l'assicurazione. Non è un caso, infatti, che l'esplosione dell'offerta di polizze di copertura del rischio *cyber* si sia verificata in concomitanza con l'innalzamento generale del livello di maturità nella gestione del rischio, in particolare proprio nel settore bancario.
Andando un po' controcorrente rispetto al sondaggio, il migliore riferimento per broker e compagnie assicuratrici per una corretta gestione del rischio *cyber* è senza dubbio il risk manager, l'unico a ricoprire il fondamentale ruolo di interprete fra business e IT in materia.
Il CIO e il CISO non possono certo autoescludersi dal problema, così come il CEO e il CFO: molto semplicemente i due mondi fanno fatica a relazionarsi con efficacia, tutto qui. Non è un caso che le normative che insistono sul settore bancario posizionino il *risk management* fra le funzioni di controllo interno e ne prescrivano il rapporto diretto verso le funzioni IT e di sicurezza delle informazioni per l'analisi del rischio informatico, verso i *business owner* per la definizione del trattamento dei rischi e verso CEO e Consiglio di Amministrazione per l'approvazione delle misure individuate.
Il compito non è semplice, perché assegnare una quantificazione economica ad impatti difficilmente misurabili, spesso intangibili, richiede una forte e diffusa cultura del rischio, competenze elevate, metodologie e strumenti collaudati, processi ben disegnati ed attuati, nonché un mandato direzionale piuttosto forte. Altrettanto arduo è il compito delle compagnie assicurative che, nell'allestimento delle polizze di copertura *cyber*, dovranno necessariamente puntare sulla flessibilità e sull'adozione di criteri di quantificazione dei molti aspetti intangibili tipici del rischio informatico.
Molto probabilmente sarà necessario attendere ancora un certo periodo di maturazione sia della cultura del rischio che dei processi di gestione del rischio *cyber*, affinché maturi anche la domanda delle aziende verso broker e compagnie assicuratrici, per coperture che siano perfettamente calzanti con il profilo di rischio aziendale e con le reali esigenze di trasferimento dei rischi residui.

2) Marco Cozzi – Responsabile IT Information Technology e D.O.R.O. Hypo Alpe-Adria-Bank S.p.A.

Uscendo dal contesto bancario in cui attualmente sono occupato e condividendo quanto scritto dal collega Ettore vorrei allargare generalizzando il white paper di Via Virtuosa al contesto delle medie e piccole imprese con cui sono in contatto grazie al ITclub FVG partendo da un affermazione:
"Nel mondo moderno la tecnologia e la globalizzazione ci permettono di rimanere connessi 24h su 24 con l'intero mondo".
Questa affermazione è ormai condivisa a livello internazionale; in questo contesto sono ancora poco considerati riguarda i rischi e le minacce per l'utente derivante dall'attuale livello di connessione, in ambito sia personale e sia aziendale.
La poca considerazione delle analisi dei rischi legati alla connessione è stata confermata anche dal "White paper di Via Virtuosa", gli imprenditori di seconda generazione ignorano i pericoli connessi alle nuove infrastrutture e spesso solo dopo la spiacevole esperienza di un "blocco effettivo" iniziano a dedicare adeguata attenzione.

La mancanza di competenze digitali è stata dichiarata anche dalla stima fatta da Confindustria durante il Fed – Forum dell'Economia Digitale [20]- ed il costo del ritardo digitale nel nostro Paese è stato valutato in circa 2 punti di Pil e in 700mila posti di lavoro non creati.

Impietosi sono anche i dati forniti della Commissione Europea il Desi [21]The Digital Economy and Society Index – riporta che il 28% degli italiani non ha mai utilizzato Internet, rispetto a una media europea del 16%. Troppo elevata, nel nostro Paese, l'ignoranza digitale, che spesso si traduce in un vero e proprio disinteresse generato dalla mancata conoscenza delle potenzialità del mezzo. L'Italia è 25esima su 28 Paesi in termini di competenza digitale generale – competenze dei cittadini, competenze delle imprese, uso dei servizi online, ecc..

Nel contesto delineato risulta difficoltoso per i responsabili IT, CIO, CISO,… confrontarsi con persone che all'interno dell'azienda abbiano adeguata sensibilità sulle tematiche trattate. La difficoltà non può che aumentare nel triveneto, con un tessuto aziendale caratterizzato da imprese medio- piccole e spesso destrutturate.

Spesso il Responsabili IT provano a rappresentare i rischi traducendo in euro il potenziale danno, per fare comprendere adeguatamente le criticità ad un CFO/CEO. Un ammirevole sforzo ma spesso non sufficiente.

I cyber-rischi sono un dato di fatto in un mondo che ruota attorno alle informazioni e ai sistemi informativi e rappresentano una sfida per qualunque azienda che utilizzi dati digitali su computer, server oppure online. Il progresso e la digitalizzazione modificano i rischi che diventano sempre più complessi.

I rischi sono di vario tipo e spaziano dalla perdita di informazioni su un unico laptop alle minacce derivanti dal cloud computing. Le aziende sono inoltre esposte al rischio di attacchi Denial of Service (interruzione dell'erogazione del servizio) o di un defacement (modifica dell'aspetto o dei contenuti) o altra compromissione del normale funzionamento dei loro siti web.

Il primo passo per comprendere dove si è più esposti ai rischi è un'autovalutazione della propria condizione di rischio.

I Penetretion Test, ovvero il processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato, dovrebbero essere fatti annualmente da ogni azienda; solo la consapevolezza della vulnerabilità dei propri sistemi consente infatti di programmare gli interventi volti a mitigare i problemi emersi..

Come scritto da Kevin Mitnick nel suo libro l'arte dell'inganno: "Un computer sicuro è un computer spento".

L'attività di" vulnerability assessment" spesso viene evitata dai reparti IT per il timore che le criticità riscontrabili mettano in discussione la propria professionalità.

Personalmente ritengo che tutte le aziende dovrebbero sottoporsi obbligatoriamente a vulnerability assessment e penetretion test, per l'infrastruttura informatica è come un "check up" per il corpo umano e rappresenta il primo passo per conoscere e valutare le criticità da affrontare.

Nella consapevolezza che i cyber-rischi non possono essere completamente eliminati, perché sussisterà sempre una percentuale di rischio residua, è importante considerare che gli effetti a catena generati possono essere attenuati ricorrendo a una combinazione di strumenti: attività di aggiornamento dei sistemi, ridisegno delle infrastrutture di sicurezza, creazione di policy e adozione di assicurazioni che coprano i rischi IT.

3) Dr. Andrea Cobelli - Responsabile Sistemi Informativi e direttore progetti ITS di ATV SRL

[20] FED – Forum dell'Economia Digitale: http://www.forumeconomiadigitale.com
[21] DESI Digital Economy & Society Index: https://ec.europa.eu/digital-single-market/en/desi

Sicurezza partecipata e divulgazione dei pericoli cyber, non vuol dire solo condivisione di regole e norme a tutela delle informazioni che viaggiano nel ciberspazio e, di conseguenza, delle infrastrutture e dei cittadini che le utilizzano. Sicurezza partecipata e cyber significa anche un ruolo attivo di tutti coloro che nel cyberspazio ci 'vivono', per lavoro o per studio.

L'evidenza della notevole frammentazione di infrastrutture non solo aumenta i costi, ma e soprattutto, indebolisce la sicurezza complessiva del sistema locale e con maggiori preoccupazioni il sistema Paese. In questo dobbiamo essere parte attiva, anzi pro-attiva.

Nelle opportunità offerte dalle analisi del Governo Italiano, si evidenzia la preoccupazione per le infrastrutture critiche. Tra esse si collocano le reti di trasporto pubblico. Sommate alle preoccupazioni per il settore pubblico, tra i più colpiti, si delinea una forte necessità di ri-progettazione globale, sia per la modellazione di piani nazionali, sia per le iniziative locali. La metodologia si traduce in impegni di pianificazione e azioni concrete in una strategia per la crescita digitale che trascini una migliore consapevolezza della cyber sicurezza.

Nel settore TPL fanno capolino gli schemi ISO 27000, con la particolare attenzione alla sicurezza del know-how aziendale e dei dati degli utenti. Quest'ultimi sono raccolti per la profilazione e per l'analisi del fruito dei mezzi di trasporto, delineando un set di dati personali potenzialmente molto delicati, a cui il Garante ha più volte prestato attenzione. La ri-progettazione dovrebbe tendere ad una maggiore uniformità dei livelli di sicurezza dei data center e degli ambienti di lavoro degli amministratori e gestori di infrastrutture critiche, sia nazioniali, sia locali, tanto più in un settore - quello del trasporto pubblico - attento alle frodi, sia interne, sia esterne, che possano drenare ricavi o colpire l'immagine aziendale.

Con la promozione, la sperimentazione, lo sviluppo delle attività operative nel cyber spazio con l'ausilio di strumenti di simulazione, con addestramento collettivo, con l'introduzione di sicurezza by default, si può efficientemente migliorare il livello degli aspetti di sicurezza.

Le analisi, l'impegno e le evidenze, devono essere distillate in una revisione dell'approccio fin qui condotto, portando i sistemi IT ad un livello superiore, non più plagiati dalle rimanenze di budget o da driver irrilevanti.

I professionisti che lavorano nei sistemi IT, hanno la responsabilità di farsi capire dal business, di guidare l'innovazione con l'aggravante di intendersi di cyber sicurezza, quasi fosse un ossimoro. Perchè spesse volte l'uno è di contrasto all'altro nel bilanciamento tra sicurezza e velocità di realizzazione, tra vincoli e inseguimento del business.

In un percorso virtuoso in continuo miglioramento, si arriva alla realizzazione di un'analisi che può portare ad arrendersi verso l'incapacità di sostenere i costi per la "completa" mitigazione dei rischi. Quando a questo si giunge, ci si approccia all'esternalizzazione del rischio e alla copertura assicurativa.

La Cyber Insurance nel confronto aperto tra IT Manager e Assicuratore

Per una migliore comprensione del tema Cyber Insurance dunque ci sembra in questa sede appropriato ed efficace cercare di rispondere alle domande poste dagli IT Manager coinvolti in questo lavoro che pur con esperienza e gradi di conoscenza differenti, presentano interessanti aspetti di convergenza tali da far supporre che le risposte possano essere considerate di interesse generale.

DOMANDA 1) Qual è il primo passo da compiere per una Azienda che si renda conto di aver bisogno di copertura Cyber?

Il primo passo da fare è confrontarsi con il proprio consulente assicurativo e chiedere una relazione sulla copertura o meno dei rischi Cyber da parte del programma assicurativo esistente. Queste le domande imprescindibili a cui la relazione deve dare risposta:

- E' prevista la Interruzione di Esercizio da indisponibilità o malfunzionamento del sistema informatico (c.d. Businness Interruption)? Se si, con che limiti?
- E' congruo il massimale previsto per la BI rispetto ai centri di costo e relativo reddito prodotto?
- Sono indennizzabili i costi di consulenza, intervento, ripristino e difesa (anche legale) conseguenti ad un evento Cyber che non coinvolga danni a cose o persone?
- Nella polizza di Responsabilità Civile Generale è corretta la descrizione della attività aziendale?
- Quali sono le esclusioni della polizza di Responsabilità Civile, con particolare focus su fornitura di servizi informatici, attività di intervento da remoto o presso terzi, fornitura/gestione di servizi PaaS, Saas, IaaS in cloud, gestione di e-commerce proprio/di terzi con relative attività di pagamento ed eventuale gestione dati di pagamento?
- Nella polizza RC Prodotti sono correttamente descritti i prodotti aziendali, specialmente se contengono firmware proprietari e se sono connessi via Internet ad altre entità?
- Dato che la polizza RC Prodotti, di base, risponde delle responsabilità previste dalla legge, la copertura in vigore è sufficiente o va ampliata?
- Quali sono le esclusioni della polizza di RC Prodotti, con particolare focus su danni immateriali o finanziari (c.d. patrimoniali puri) ed esclusioni specifiche riguardanti il mondo IT?

DOMANDA 2) Esistono condizioni vincolanti ai fini della assicurabilità? (p.es. certificazioni, ...) ovvero le Assicurazioni valorizzano e tengono conto delle attività di mitigazione del rischio o aumento della resilienza (tecnologica, di processo, formazione del personale, organizzativa) nel definire/rinegoziare un premio?

Da parte degli assicuratori non vengono posti, al momento, particolari vincoli.

Unica richiesta è di essere "conformi alle norme di legge". In Italia, la normativa che impatta i sistemi informatici è quella relativa alla gestione dei dati sensibili (c.d. Legge sulla Privacy), che diventerà ancora più importante nel 2018 con l'adozione automatica del GDPR, Regolamento Europeo sulla Privacy.

La valutazione di assumibilità o meno del rischio, nonchè la sua quotazione, avviene tramite un questionario diverso e proprietario a seconda del contratto assicurativo considerato. Non esiste un questionario "normalizzato" in ambito cyber, come non c'è in altri ambiti.

Eventuali certificazioni presenti in azienda (ISO 27001/2), pur non obbligatorie, sono benvise dagli assuntori, così come l'adozione di *best practices* - ad esempio l'esecuzione di penetration test, l'esistenza di piani formalizzati di *disaster recovery* o *businness continuity* - possono portare a condizioni di copertura più favorevoli, quali l'aumento dei limiti di risarcimento, la riduzione delle franchigie contrattuali e la riduzione del premio annuo.

DOMANDA 3) Il nuovo Regolamento Europeo della Privacy – GDPR è portatore di alcune novità che promettono di impattare in modo significativo sulle imprese colpite da un cosiddetto "Data Breach" e non solo. Una polizza Cyber è in grado di ridurre questo impatto?

Il GDPR che entrerà in vigore nel 2018 amplia le definizioni di ***Data Breach*** e di **Dato Personale** e dunque cresce la platea delle aziende che detenendo questo genere di informazione dovranno essere *compliant* o saranno costrette alla *disclousure*:

Per **dato personale** si intenderà qualunque tipo di informazione che permetta di identificare una persona online, quindi anche un indirizzo IP, dati di geolocalizzazione oppure pseudonimi saranno considerati dati sensibili.

Mentre ora per ***Data Breach*** si intende la "perdita" di dati, fra due anni la definizione sarà estesa a distruzione, alterazione, pubblicazione non autorizzata o anche semplice accesso a dati personali. La gamma degli eventi che ricadono sotto il controllo del GDPR è dunque molto più ampia.

Tra l'altro le sanzioni potranno scattare anche se non si è *compliant*, non solo in caso di *data breach* e riguarderanno i dati sensibili di cittadini europei ovunque nel mondo essi vengano gestiti, ovvero il braccio del Garante si estende alle aziende multinazionali europee e non.

Anche la base di rischio per il business si allarga:

Rischio reputazionale: le aziende – che dovranno comunicare il data breach al Garante e in certe circostanze agli individui i cui record sono stati colpiti entro 72 ore dall'accadimento – saranno esposte a un pesante diminuzione della reputazione e quindi del patrimonio netto.

Rischio finanziario: la non compliance al GDPR espone le aziende a sanzioni pesanti e potenzialmente pari al 4% del fatturato annuo (aggregato, se l'azienda ha più sedi in tutto il mondo) con un tetto massimo di € 20 Mln.

Fatta questa premessa, sul piano assicurativo, sarà importante dichiarare in polizza se si detengono dati di questo tipo e in quale paese e quali misure si prendono per difendersi dal *data breach*.

Attualmente in Italia la polizza non fa fronte alle sanzioni che ci dovessero essere comminate, ma **può coprire le spese legali, i costi di comunicazione imposti dalle Autorità competenti ed i costi per la ricostruzione e il**

monitoraggio della reputazione dell'assicurato e delle persone danneggiate. Queste voci sono generalmente incluse tra i costi per il cosiddetto Incident Response, anche in assenza di richiesta danni da parte del Terzo.

Se un Terzo gestisce per mio conto Dati Sensibili, dovrò innanzitutto verificare i contratti che regolano il rapporto con il fornitore terzo, poichè la richiesta danni in caso di Data Breach su sistemi non gestiti direttamente sarà possibile solo per via legale. Ovviamente sarebbe molto utile sapere anche come il mio fornitore è assicurato per la responsabilità a lui afferente.

DOMANDA 4) Quanto e cosa è possibile mettere in copertura? I rischi assicurabili

Premesso che i contratti Cyber presentano importanti differenze per voci assicurate, definizioni ed esclusioni, possiamo individuare 5 grandi famiglie di rischi assicurabili: Danni materiali (diretti ed indiretti), Danni Immateriali, Danni da Interruzione di Esercizio, Costi e Richieste di Risarcimento di Terzi. Vediamo la loro corrispondenza con le voci previste in un generico contratto Cyber.

a) 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, allagamento, 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". Particolare attenzione va prestata alla eventuale esclusione degli eventi catastrofali (terremoto, alluvioni ed allagamenti), presente in molte polizze All Risks. **I danni materiali e diretti possono anche non essere previsti nella Polizza Cyber,** se si è provveduto alla corretta strutturazione delle coperture assicurative tradizionali.

Danni materiali indiretti (o consequenziali)

Si tratta ugualmente di danni a beni materiali, ma conseguenza indiretta di danni. Ad 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.**

b) Danni immateriali

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 (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*) può distruggere o compromettere l'integrità di un software e/o l'insieme logico di informazioni, rendendo indisponibili i miei dati aziendali. Ciò innesca una serie di eventi che possono avere come conseguenza danni di natura economico/finanziaria (c.d. danni patrimoniali puri) come ad esempio la perdita di credibilità per un marchio conosciuto, il "salto" di una campagna di

vendita, etc. Il danno immateriale, ovvero il risarcimento per la distruzione di un dato, non fa parte attualmente delle partite oggetto di risarcimento.

c) Danni da Interruzione di Esercizio

Questa è una categoria a cavallo tra **danni e costi**. In questa voce, di solito, viene indennizzatala perdita di profitto lordo (o margine di contribuzione), tutti i costi cosiddetti "fissi" o non cessanti in caso di sinistro e gli extracosti che mi trovo a sostenere per continuare la mia attività.

Nella pratica, in caso di fermo di attività per evento Cyber, in particolare per attività molto sbilanciate verso attività di e-commerce o che trattano con la GDO (Grande Distribuzione Organizzata), il mio bilancio risente immediatamente del calo dei ricavi e della persistenza o aumento del livello dei costi. I canoni di leasing, ad esempio, sono considerati un costo "fisso", come gli stipendi dei dipendenti. Extracosto indennizzabile, sempre a titolo di esempio, sono considerati gli straordinari o i costi sostenuti in emergenza per il ripristino dell'operatività. Il prevedere una copertura assicurativa per i danni da Interruzione di Esercizio può determinare la **sopravvivenza** o meno dell'azienda.

d) Costi

E' la categoria più facile da assicurare. Sono tutti i costi sostenuti a piè di lista per reagire alla problematica Cyber. Qui di seguito un elenco dei principali costi indennizzabili:

- Costi per Consulenza
- Consulenza di crisi
- Consulenza per Pubbliche Relazioni
- Consulente di Reazione
- Costi di Difesa
- Costi di risposta
- Spese per Pubbliche Relazioni
- Costi (spese) per ripristino (dei dati)
- Servizi di pronto intervento informatico
- Spese di Gestione della Crisi
- 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.

e) Richieste di risarcimento

Una interruzione di servizio, una diffusione di dati sensibili, un errore di programmazione o di intervento ICT possono dare origine ad una richiesta di danni da parte di Terzi. E' un campo ben conosciuto dagli assicuratori e affrontato nelle polizze di Responsabilità Civile Generale o Responsabilità Civile Professionale.
A seconda della prevalenza e pervasività dell'attività Cyber nell'attività e prodotti aziendali, la richiesta di risarcimento sarà trasferibile a una delle coperture suddette. Ultimamente anche la polizza RC prodotti puo' essere interessata da problematiche legate al mondo IoT.

Per meglio chiarire quanto sopra possiamo attingere alla cronaca[22]:
Un articolo del 2015 riuniva una serie di "sinistri" accaduti nel Trevigiano e di pubblico dominio: Geox, La Contarina, Benetton colpiti da Ransomware.
Comuni i problemi: attività informatica paralizzata, tecnici al lavoro, disagi e tempi morti sul lavoro, richiesta di riscatto. Nel caso di Benetton poi il malware inoculato ha permesso di "clonare" una intera collezione di abiti che in seguito si è scoperta essere finita in vendita all'estero in negozi non autorizzati. Fermo d'attività, costi di ripristino IT e della reputazione sarebbero state probabilmente ottimi *trigger* di polizza.
Un esempio diverso è quello del caso occorso alla Mattel, notissima casa produttrice di giocattoli americana[23]. Tutto sarebbe partito da una email il 30 aprile 2015, quando al direttore finanziario della Mattel arriva un messaggio di posta elettronica dall'indirizzo del nuovo CEO. L'oggetto della mail è un ordine di effettuare un pagamento da 3 milioni di dollari per un nuovo fornitore cinese. Dopo la validazione il pagamento parte. I soldi verranno poi recuperati perché in Cina ci sono stati tre giorni di chiusura e al primo giorno lavorativo una squadra anti-frode va a congelare il conto del destinatario.
In questo caso, l'eventuale perdita di denaro non sarebbe stata indennizzabile. Non c'è stata una violazione della rete o una modifica di dati aziendali, ma solamente l'applicazione di una tecnica di ingegneria sociale.
La fattispecie infatti, ovvero il trasferimento di fondi non autorizzato e non recuperabile, è presente in uno solo dei contratti assicurativi fino ad ora analizzati e lo considera come conseguenza di un "Furto IT" che corrisponda alla seguente definizione:
"Furto IT significa ogni intrusione mirata di qualsiasi Terzo all'interno del Sistema Informatico della Società che si traduca nella cancellazione fraudolenta e non autorizzata o nell'alterazione di Dati contenuti nel Sistema Informatico della Società."
La conseguenza di un Furto IT quindi è assicurabile qualora ci sia una violazione dei sistemi informatici dell'Azienda.

DOMANDA 5) Quali di questi rischi è possibile coprire subito e quali hanno bisogno di una revisione dei processi aziendali?

I rischi sopra descritti sono da subito trasferibili all'assicuratore specializzato. Tuttavia la dinamicità e mutevolezza del rischio Cyber impongono che in Azienda sia attuato un processo continuo di analisi e miglioramento senza tralasciare le piccole problematiche. Gli esiti di questo processo servono come input per la trattativa con il partner assicurativo. Il livello di analisi, mitigazione, controllo dei reali rischi cyber-correlati e la valutazione dell'impatto finanziario permetterà

[22]http://tribunatreviso.gelocal.it/treviso/cronaca/2015/03/12/news/hacker-all-attacco-di-contarina-violati-dati-e-archivi-1.11030528
[23]http://www.corriere.it/esteri/16_marzo_29/cina-mattel-truffa-colpo-grosso-marchio-rosso-tre-milioni-7034267c-f5b3-11e5-a42a-1086cb13ad60.shtml

al management di programmare interventi di mitigazione e controllo del rischio che permettono di assicurarsi meglio nel merito delle coperture da richiedere o escludere, degli importi per cui assicurarci o delle franchigie che possiamo accettare.

DOMANDA 6) E' vantaggioso frazionare il rischio su più compagnie e prodotti assicurativi?

Essenzialmente solo in caso di contratti per i quali un singolo assicuratore non abbia una capacità assuntiva sufficiente, ovvero i limiti di risarcimento richiesti dalla specifica attività siano molto elevati. Va comunque verificata la posizione assicurativa dell'azienda in analisi, poichè l'eventuale sovrapposizione di contratti assicurativi non aumenta necessariamente l'efficacia complessiva dell'assicurazione.

DOMANDA 7) Posso scegliere liberamente a chi affidare le attività di risposta ad un eventuale sinistro cyber e come devo documentare queste attività/costi? Le assicurazioni prevedono servizi inclusi nel premio assicurativo (tutela legale, unità di crisi, call center, periti esperiti in security & forensics)?

Su questi aspetti c'è ampia flessibilità.

Le attività svolte andranno concordate e comunicate di volta in volta alla Compagnia e l'Assicurato potrà scegliere il partner più appropriato.

Alcuni assicuratori mettono a disposizione *hot lines* disponibili e consulenti esperti disponibili h24 per una immediata e professionale gestione del sinistro.

La documentazione prodotta poi normalmente consta di una relazione su quanto svolto, preventivi e relative fatture a chiusura dell'attività. Fondamentale è essere affiancati da professionisti assicurativi che seguano e curino la comunicazione con la Compagnia di Assicurazione.

DOMANDA 8) Come è possibile mettere in copertura le nuove minacce che si evolvono quotidianamente e al momento della stipula non ancora note?

Il linguaggio assicurativo normalmente è sufficientemente ampio da poter comprendere in maniera automatica nuovi rischi che dovessero sopravvenire.

In questo senso è molto importante leggere le cosiddette "esclusioni" di polizza che rappresentano, in maniera immutabile, ciò che la polizza non indennizza.

DOMANDA 9) E' opportuna una revisione periodica oltreché annuale?

Attualmente la revisione periodica/annuale non è richiesta dagli assicuratori, ma su rischi di una certa complessità dovrebbe far parte del processo di Cyber Risk Management gestito dal Risk Manager. In sua assenza, è necessario un tavolo aziendale condiviso convocato periodicamente dal CIO ed al quale l'Assicuratore dovrebbe essere convitato.

DOMANDA 10) Nelle revisioni è consigliabile considerare gli incidenti avvenuti e i "mancati incidenti"?

Nel caso si stipuli una polizza o si cambi assicuratore, è obbligo di legge dichiarare gli incidenti avvenuti che abbiano avuto un qualche impatto economico.

Il tavolo aziendale prima nominato serve invece al processo di analisi continua che deve essere presente in Azienda per l'immediata identificazione di nuove minacce e criticità. La metodologia SixSigma (Motorola) insegna che piccoli problemi possono sommarsi e creare un grosso problema.

DOMANDA 11) Quali sono gli strumenti per valutare la copertura e il fornitore?

Le compagnie assicurative con prodotti specializzati ed esperienza non sono molte sul mercato italiano, e con prodotti molto diversi tra loro. Affidarsi dunque all'analisi da parte di un **intermediario assicurativo specializzato e con esperienza** diventa fondamentale per la valutazione della adeguatezza del prodotto assicurativo.

DOMANDA 12) Ci sono parametri standard che possano aiutare il confronto tra fornitori?

Il mercato delle polizze specifiche riguardanti il Cyber Risk è molto ristretto e recente. Le soluzioni Cyber per rischi di un certo livello sono estremamente personalizzate e per questo difficilmente comparabili.

Nella lettura delle garanzie, particolare attenzione deve essere posta sulle **definizioni di polizza**, che ne definiscono ampiezza di copertura e condizioni di attivazione, e sulle **esclusioni**.

DOMANDA 13) Le compagnie assicuratrici, nell'allestimento dell'offerta di coperture del rischio cyber, hanno pensato ad introdurre criteri di flessibilità che consentano loro di adattare le coperture alle specifiche esigenze delle aziende, ovvero ai rischi residui da trasferire da queste identificati, tenendo conto che ciascuna azienda ha proprie peculiarità in termini di cultura, governo e propensione al rischio?

Sì. I testi Cyber Risk attualmente proposti sono altamente personalizzabili. La compilazione di un questionario assuntivo deve essere solo il punto di partenza per il trasferimento del rischio. La personalizzazione delle garanzie offerte, loro analisi e presentazione ai *risk owners* aziendali è fondamentale per valutare l'adeguatezza della copertura assicurativa scelta.

DOMANDA 14) Quali criteri sono stati definiti e/o adottati dalle compagnie assicuratrici per una copertura efficace dei danni intangibili, come il danno reputazionale o la perdita di posizione sul mercato, che potrebbero manifestare effetti dilazionati e prolungati nel tempo e, nei casi più gravi, risultare irreparabili?

Due parametri di valutazione:

- costi di intervento da parte di consulenti reputazionali e/o di comunicazione;

- perdita di profitto/margine di contribuzione dovuta all'evento Cyber.

Come si può intuire, sono criteri di valutazione oggettivi. I costi vengono riconosciuti a piè di lista e, tramite un analisi di bilancio pre e post evento, si valuta l'impatto negativo dello stesso sul Conto Economico e quindi il risarcimento dovuto.

Diversa, e non indennizzabile, la "perdita di valore" del marchio o la perdita di *know how*. E' una pura componente patrimoniale non oggetto di copertura nei contratti Cyber visti fino ad ora.

DOMANDA 15) Quali ruoli aziendali sono attualmente i principali interlocutori per le società broker e le compagnie assicuratrici in materia di rischio cyber e di copertura assicurativa dei rischi informatici da trasferire?

In Italia, l'agente di assicurazioni e il broker assicurativo solitamente trattano direttamente con la proprietà aziendale, con l'ufficio acquisti o con il CFO. Troppo spesso ancora si sente la mancanza del Risk Manager che si faccia portatore delle istanze aziendali con uno sguardo a tutto tondo e una maggiore consapevolezza delle correlazioni di rischio e che non sia il semplice “valutatore di polizze”.
Come è stato precedentemente messo in risalto sarebbe auspicabile – ed è nei fatti raro - un confronto con altre figure aziendali quali, ad esempio, il CIO ed il Direttore di Produzione. Aspetti interessanti per la definizione del rischio possono essere messi a fattor comune anche dai Direttori Marketing e Commerciali che gestiscono attività *internet based* e hanno intensi scambi di informazioni col mondo esterno a mezzo posta elettronica e device mobili oltre a essere spesso driver di innovazione digitale.
Particolare rilievo sta assumendo l'ambito **IoT**. Tali oggetti iperconnessi alla rete, infatti, sono la perfetta fusione tra il rischio cosiddetto "analogico" e quello "digitale". Sono infatti oggetti fisici, che interagiscono con il Cliente finale ma che **comunicano all'esterno e/o tra loro in maniera indipendente**. Per l'analisi dei rischi connessi a questa tipologia di oggetti, spesso CIO, project manager e responsabile di produzione devono sedersi allo stesso tavolo.

DOMANDA 16) Posso assicurarmi contro la perdita di dati “miei” affidati a un Terzo colpito da data breach o altro problema?

In questa ottica, prima di tutto vanno analizzati i contratti in essere con i fornitori ed eventuali manleve presenti che possono fortemente limitare la possibilità di una azione di responsabilità verso il terzo. I servizi in cloud, molto spesso sono esclusi dalle coperture o comunque oggetto di analisi specifica da parte degli assicuratori.

Se ho acquistato un software che mi causa un problema in azienda, dovrò valutare di rivalermi sul fornitore per il “prodotto difettoso” e i danni che ha causato. Sarà un problema suo verificare se si è adeguatamente coperto, altrimenti in caso di causa legale che riconosca il suo torto dovrà provvedere direttamente.

DOMANDA 17) Esiste una copertura per la perdita del dato, per il danno economico causato dalla perdita del dato?

Non c'è contratto assicurativo, almeno fino ad ora, che preveda una valorizzazione patrimoniale del "dato" e quindi un eventuale risarcimento causato dalla sua semplice indisponibilità o perdita.

Sono invece indennizzabili le conseguenze economiche, in termini di *businness interruption,* o i costi sostenuti per attività a difesa della reputazione/marchio aziendale.

DOMANDA 18) E il ransomware?

Esistono tutele assicurative attivabili per far fronte sia al riscatto, derivante ad un attacco da *ransomware,* che al ricatto a cui si è sottoposti da un attaccante che minaccia il corretto svolgimento della attività aziendale.

Lettura dei risultati del Survey, sintesi e raccomandazioni da parte dell'Assicuratore

Per concludere questo certo non esaustivo, ma ci auguriamo chiaro, primo approccio all'outsourcing assicurativo ci sembra di poter dire che sul **fronte delle imprese** una **costante e migliorativa gestione della sicurezza ICT** nel senso più ampio,insieme ad un **corretto trasferimento del rischio residuo** (posto che questa "residualità" sia stata efficacemente individuata) siano da considerarsi strettamente correlati ed imprescindibili.
Altrettanto imprescindibile è il **contributo che i risk owner di Businness Unit** possono dare per definire lo stato di rischio, perché possono dire quale infrastruttura, software, device, dato sono critici per la loro attività ed aiutare nell'analisi dell'impatto che un evento Cyber che li colpisse possa avere sulla produttività.
Deve crescere la consapevolezza di un tema fin qui poco affrontato assicurativamente che è quello della copertura della **Business Interruption o Fermo d'Attività**. Se nel mondo "analogico" solo il 12% delle aziende assicurate All Risks-Incendio decidono di attivare la polizza BI ad essa correlata con grave danno per la competitività e la stessa sopravvivenza dell'azienda, nel mondo "digitale" questo ci appare ancora più pericoloso poichè un evento Cyber può avere conseguenze immediate, trasversali e pervasive anche a livello geografico.
Altro aspetto su cui porre attenzione sempre ed in modo particolare in ottica cyber, è quello del controllo dei **contratti in essere con i nostri fornitori, incluse le loro coperture assicurative di RC.**
La complessità del tema e dell'analisi dell'offerta sul mercato assicurativo rileva inoltre che sul campo sono molto pochi gli attori esperti, sia da parte delle Compagnie che, in particolare, dei professionisti che operano in qualità di intermediari autorizzati. Le risposte più adeguate arriveranno da interlocutori altamente specializzati e con provata esperienza sul campo. D'altro canto è chiaro che a fronte di istanze chiare e precise poste da aziende più consapevoli e proattive**, il mondo assicurativo debba fare uno sforzo importante** per affinare l'offerta, renderla più capace di rispondere alle reali/ipotizzabili esigenze delle aziende e naturalmente contemplare processi di adeguamento snelli ed efficaci al mutare delle situazioni.
Se fin qui abbiamo provato a delineare le premesse per il migliore dei mondi possibili, vediamo lo stato dell'arte guardando con occhio critico agli **esiti della survey** che è alla base di questo documento e che aveva lo scopo di registrare il grado di sensibilità e preparazione delle aziende, nella persona di quello che è in Italia, a torto o a ragione, il più "esperto" interno in materia di rischio ICT , anche se quello, almeno ad oggi, meno interpellato quando si tratta di assicurazioni, l'IT Manager.

I risultati della Survey

Il campione, che si è delineato sulla base di tre caratteristiche Fatturato, Settore e numero dipendenti, vede prevalere il settore industria e servizi (rispettivamente il 40% e 35%) al di sopra di 20 Mln Euro di fatturato (75%) e con più di 100 addetti (50% tra 100-500 e 30%> di 500).
Questo ci fa presumere che aspetti come la Reputazione, il fermo d'attività (in amministrazione come in produzione) e la gestione dei dati sensibili possano essere aspetti critici.
La survey ha richiesto in prima istanza agli IT Manager quale allo stato dell'arte sia il committment del board alla creazione di un tavolo sulla sicurezza aziendale e se la sicurezza ICT venga vista come parte integrante del tema sicurezza generale o possibile fonte di costi e danni (quesito 1,4). Quindi gli abbiamo chiesto di compiere quello che probabilmente è un passo insolito: interfacciarsi con il collega CFO o con la proprietà per poter rispondere al quesito sulla presenza o meno di alcune coperture in azienda (quesito 3).

Prevale con un 60% la risposta positiva sul fatto che il CIO venga integrato in azienda in un approccio ampio di security, mentre nell'andare a vedere i dettagli del tipo di cause collegate ad incidenti informatici, si deduce che incidenti se ne verificano e che sostanzialmente essi sono riconducibili in misura pressoché equa all'attacco (esterno/interno), all'errore umano (interno/esterno) e al guasto (q. 1 e 4). Il 39% dichiara di essere a conoscenza di sinistri avvenuti negli ultimi 5 anni e che nella maggior parte dei casi si tratti di ransomware (q. 9)

Nel 60% dei casi il CIO non si è interessato fin qui delle coperture assicurative (q.2) e seppure nell'80% dei casi nessuno in azienda è venuto a chiedergli ipotesi di impatto di un sinistro (q. 4), egli ne ha ben chiara l'origine (q. 4) ed è in grado di indicare quali settori aziendali/business unit sono critiche per l'azienda e potrebbero soffrire di più di una interruzione d'attività (q 8).

Evidentemente il CIO si occupa di sicurezza informatica, ma ci si occupa poco di formalizzare delle procedure/policy (28%) o modellizzare le problematiche (12%) probabilmente per scarso committment a una visione di risk management. Spesso invece attua un controllo delle vulnerabilità (60% dei casi). Altrettanto positivo è che al CIO pervengano sollecitazioni o richieste di informazione in merito alla gestione della sicurezza ICT (q.7) in primis dall'interno (+70%) quindi da auditor esterni (+ 28%) e poi dai clienti e dai fornitori ICT a pari merito (23-24%). In questo campione, che possiamo definire in ottica Cyber Security come "virtuoso", si attuano piani di Business Continuity e Disaster Recovery nel 50-60% dei casi. Anche la consistenza di sollecitazioni interne o da parte dei clienti sono un segnale importante che ci siano buone premesse per strutturare un percorso di Cyber Risk Management. Meno ci si preoccupa di approntare unit interne o esterne per la gestione di una eventuale crisi reputazionale (18%). Questo fa concludere a una prima istanza che i virtuosi possono presentarsi come tali al tavolo assicurativo e "contrattare" alcuni termini della copertura per trasferire appunto **un rischio residuo** soprattutto da **fermo d'attività** e da Ransomware ma, ove la reputazione fosse un elemento importante non gestito, dovrebbero investire di più su quanto i contratti assicurativi prevedono riguardo la copertura del **danno reputazionale**.

Per chiudere, possiamo tornare al valore e alla funzione dell'outsourcing assicurativo, una copertura finanziaria utile e importante. Dal quesito 8 emerge che nella visione del CIO gli impatti più pesanti di un fermo di attività ICT si verificherebbero su Amministrazione/fatturazione (+ 80%), logistica e consegne (73%) e vendite (60%).

Se non fatturo o non sono in grado di pagare le fatture fornitori ho un danno economico e reputazionale, se non ricevo ordini ho un danno economico e probabilmente un tasso di abbandono clienti (è pericoloso non mettere un cliente in condizione di richiedere quello che desidera) che si verifica anche nel caso di problemi logistici. Tutte situazioni che causano cali di fatturato e buchi di bilancio nel breve, medio e lungo periodo.

Per rendere evidente questo concetto, che riteniamo una leva importante all'approccio GESTITO del Cyber Rrisk, in conclusione riportiamo due esempi frutto di una case reale e di una modellizzazione semplificata:

Trattasi di una azienda alimentare che produce a marchio proprio e commercializza prodotti BIO, con 15 shop in italia per la vendita dei prodotti e uno shop online che insieme producono 90 Mln di Euro di fatturato annuo. Questa azienda subisce un lungo "sniffing" e studio delle procedure aziendali grazie ad un malware inoculato via mail in maniera inconsapevole, una sostituzione di IBAN per dirottamento di pagamenti ai fornitori e poi il furto di dati delle carte di credito degli acquirenti online che portano a lamentele dei clienti e a fermo dell'e-commerce.

Il sinistro complessivo di 3 Mln si traduce in due principali componenti: **costi diretti** e **fermo di attività**.

Il ROE nella tabella sottostante è stato scelto come indice riassuntivo perché include anche la parte finanziaria del bilancio, ovvero quelle componenti non strettamente legate alla gestione caratteristica. Se, ad esempio, è stato contratto un prestito/mutuo per sopperire al problema, il ROE ne tiene conto. Come tiene conto dei costi di investigazione, risposta, etc.

In questo caso la ditta NON era pronta né in ottica di gestione della sicurezza, né assicurativamente. Ha dovuto reagire in emergenza ed ha subito totalmente l'impatto (fermo di circa 15gg, tre mesi di riallineamento).
Ovviamente, in emergenza, tutto costa di più. Ripartizione di circa 400K Eur in costi di reazione ed il resto di BI.
Da notare: la BI, pur essendo "corta" (tre mesi complessivi), ha un riflesso pesantissimo sul bilancio annuale.

Indici	Post sinistro	Pre sinistro
ROE	-4,58%	23,97%
Valore aggiunto	18,78%	22,80%
Utile (perdita)	(-481.000 Eur)	2.600.000 Eur
Margine di Contribuzione	25.600.000	27.170.000

Questo è invece l'esito del sinistro considerando che l'azienda sia virtuosa in ottica della sola cyber security (inclusa formazione del personale e gestione della reputazione) o che abbia anche provveduto a tutelarsi assicurativamente in modo appropriato.

Indici	Pre sinistro	Post sinistro (no ass)	Post sinistro (ass)
ROE	21,28%	13,67%	21,12%
Valore aggiunto	21,75%	20,90%	21,69%
Utile (perdita)	2.300.000 Eur	1.436.000 Eur	2.250.000 Eur
Margine di Contribuzione	27.000.000	26.400.000	26.900.000

CONCLUSIONI

Si accenna che il Cyber Risk è troppo grande per essere coperto con una assicurazione[24]. Dal presente documento emerge che, parlando di Cyber, serva definire meglio la comunicazione fra IT Manager e Assicuratore. Per cui l'IT Manager deve comprendere cosa chiede l'Assicuratore e quest'ultimo deve capire cosa serve all'IT Manager.

Se si adotta una strategia di mitigazione del Rischio Cyber, per prima cosa bisogna capire la situazione e porre rimedio ove possibile. Il Rischio Cyber che va coperto con una assicurazione è quello residuo quando si sono mitigate le vulnerabilità risolvibili, evidenziate da una analisi. I due percorsi possono comunque andare in parallelo

Il costo di un incidente informatico non è solo costituito dalla perdita diretta (inoperatività, sostituzione di Hardware, ripristino dei dati…) ma è anche fatto di perdite indirette (danno di immagine, costi di investigazione, scelte sbagliate in stato di emergenza…). Qui credo ci sia la maggior carenza di un IT manager e cioè quella di tradurre in costi benefici una strategia coerente sulla Cyber Security anche in ambiti di cui non ha competenze. Qui spero che il lavoro abbia dato un contributo agli IT Manager che lo leggeranno.

Se il primo passo per una azienda è capire la propria situazione nella sicurezza informatica, questa misurazione può costituire il protocollo di intesa fra IT Manager e Assicuratore. La misurazione oggettiva e la strategia di mitigazione del Rischio Cyber deve identificare il rischio residuo trasferibile all'assicuratore. Questo ove possibile in particolare se il Rischio Cyber residuo è grande e non prevedibile. Se l'azienda è una infrastruttura critica (IC) questa polizza dovrebbe diventare un obbligo. Poiché le possibili vittime non avrebbero sufficienti risorse per gestirne le conseguenze.

Solo se si adotta una politica di continuo miglioramento sulla sicurezza informatica il rischio residuo da assicurare può essere trasferito assicurativamente. Le polizze dovranno essere soggette ad un processo di revisione, totale o parziale con una frequenza almeno pari a quella con cui si aggiorna una analisi della sicurezza informatica.

[24] https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de