"Cyber Risk e Cyber Risk Insurance"

Sfida assicurativa al CIO referente della Cyber Security Effectiveness aziendale

A cura di Cesare Burei – Margas

Focus ON tratto dal

Prendi visione del contenuto su https://clusit.it/rapporto-clusit/

Richiedi il rapporto completo a rapporti@clusit.it

Cyber Risk e Cyber Risk Insurance

Sfida assicurativa al CIO referente della Cyber Security Effectiveness aziendale

In attesa che i Risk Manager aziendali competenti in materia di Rischi Cyber, e non sono ancora molti, entrino in azione a tutti i livelli di imprese, a chi si può affidare la gestione del Cyber Risk e in particolare l'aspetto del trasferimento del rischio alle Assicurazioni? La risposta è in un tavolo collaborativo che ha nel CIO il suo volano.

Nel Report Clusit 2016 con un Focus On dedicato allo strumento assicurativo a supporto dellagestione del cosiddetto Cyber Risk, si sono datele indicazioni basilari su terminologia, aspetti chiave ed utilità delle polizze cyber. Gli autoriimplicitamente si rivolgevanoal CFO, figura che di solito sovraintende all'aspetto assicurativo in azienda.

A distanza di un annoil confronto quotidiano tra le aziende, i broker assicurativi e i consulenti ICT ha messo in evidenza questi elementi:

- Il Rischio Cyber comprende l'incidente/attacco e tutte le conseguenze dirette e indirette che questo comporta
- E' aumentata la consapevolezza della pervasività del Rischio Cyber ben oltre le mura dell'EDP in un ecosistema digitale fatto di interconnessioni e interdipendenze di processi, persone e ora anche oggetti (IoT)
- Si parla sempre più di Gestione del Rischio: analisi, mitigazione e trasferimento assicurativo
- La business Interruption, la reputazione e la perdita/indisponibilità dei dati sono le maggiori preoccupazioni delle aziende.

Nasce da qui una doppia indagine fatta nel Nord-Est e confluita in "Enterprise Cyber Risk Exposure & Insurance"[1]di Via Virtuosa in collaborazione con Margas per la parte assicurativa, pubblicata online a fine 2016 e che per brevità qui chiameremo d'ora in avanti "Whitepaper".

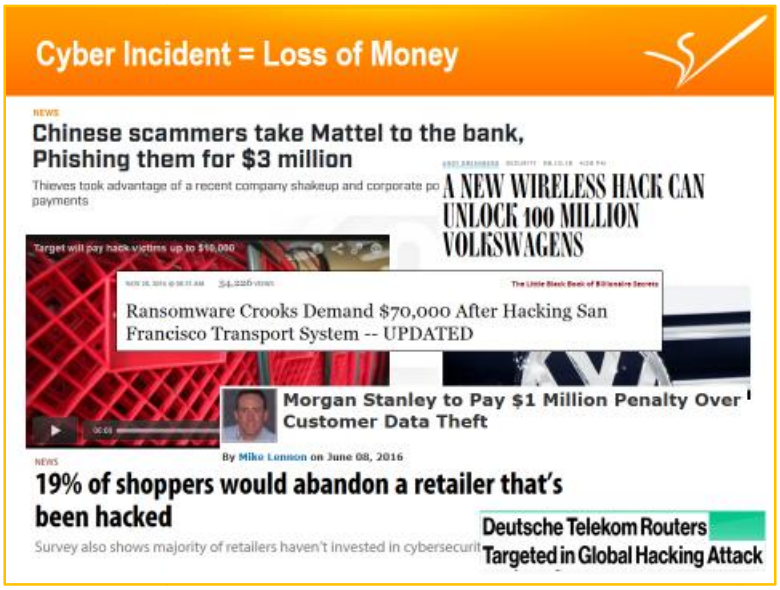
La prima indagine, attraverso le risposte di CIO e Amministratori di Sistemi, disegna**l'esposizione al rischio** da parte delle imprese affinché CFO e CEO possano rendersi conto della centralità dell'attività di Cyber Security gestita internamente o trasferita ai fornitori. La seconda indaginesempre svolta con l'aiuto del CIO in quanto detentore della dimensione del rischio o dei livelli di protezione messi in atto, cerca di prendere il polso del livello di **conoscenza e sensibilità rispetto al tema del trasferimento assicurativo**.

I risultati mettono in luce alcuni aspetti che conferiscono al **CIO un ruolo chiave** nella fase di transizione dalla gestione della ICT security al **cyber risk management** aziendale di cui il trasferimento assicurativo del cosiddetto "rischio residuo" è una componente ultima, ma fondamentale. Per questo il whitepaper includealcune informazioni di base sul mercato assicurativo italiano e soprattutto, grazie alle a 18 domande che tre CIO si sono prestati a porre, 18 utili risposte per orientarsi in modo più consapevole nel percorso operativo di acquisizione dello strumento assicurativo.

[1]*Il Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance" è frutto del lavoro congiunto di Luca Moroni di **Via Virtuosa**, Auditor e Broker di servizi di Cybersecurity e IT Governance, e Cesare Burei di **Margas**, Broker e Consulente di Assicurazioni, socio Clusit e docente Cineas. Contiene anche i contributi dei CIO E. Guarnaccia – BPV | M. Cozzi – Hypo Bank |A. Cobelli – ATV| e le risposte alle loro 18 domande sulla cyberinsurance. La survey sull'esposizione al rischio si è svolta nel triennio 2013-2016, quella sulla Cyber Risk Insurance nell'estate del 2016. Il Whitepaper è gratuitamente scaricabile da: www.viavirtuosa.com/whitepaper e sostiene il Progetto di rilevazione "Generazione Z" per la sicurezza online e la prevenzione dei rischi dei minori https://www.facebook.com/ProgettoGenerazioneZ/

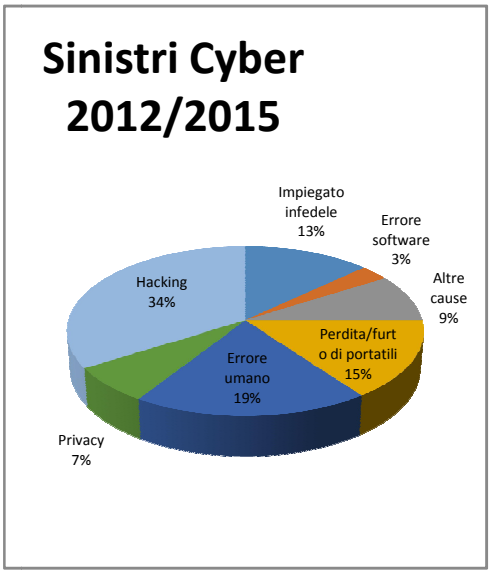
Cyber Risk Insurance. Perché?

La certezza di non potersi difendere completamente dal Cyber Risk, impone la sua gestione e una corretta valutazione degli strumenti necessari, del loro costo e dei benefici che questi apportano. In estrema sintesi, è una questione di equilibrio tra l'impatto di un sinistro cyber o cyber-correlato, i soldi investiti nel processo di gestione/assicurazione e mantenimento delle marginalità aziendali.



Fonte: L. Moroni - Presentazione Whitepaper "Cyber Exposure & Cyber Risk Insurance" Infosek 2016 - Slovenia

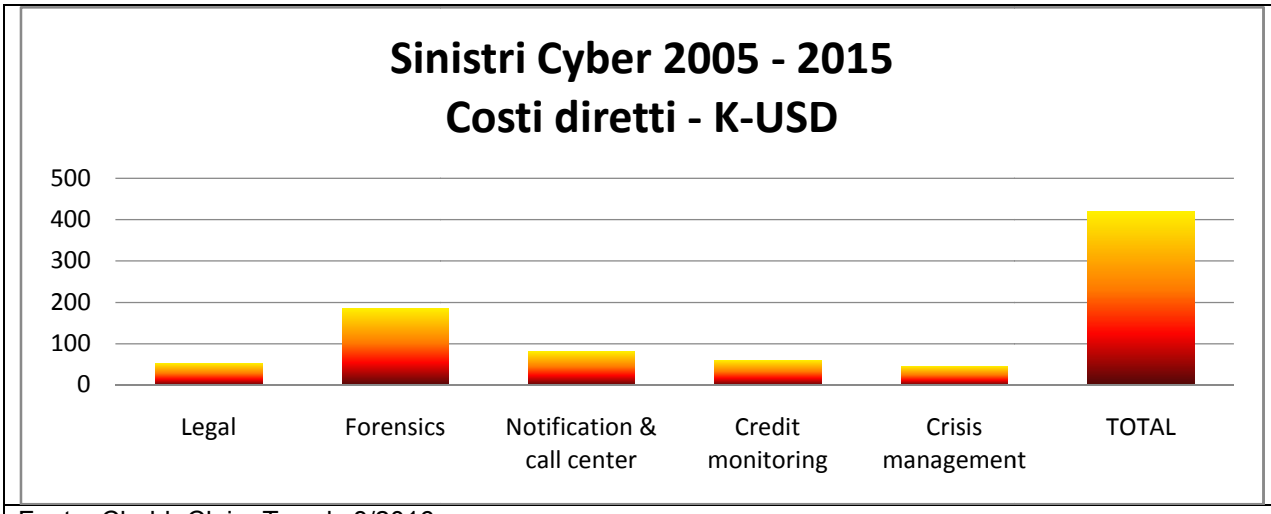
In occasione del Security Summit e tramite il Clusit Report vengono date tante cifre e tante percentuali che descrivono il panorama della in-sicurezza cyber,evidenziando che la Sicurezza 100% non esiste.



Fonte: CHUBB Claim Trends 8/2016

Quello che è possibile fareè essere Proattivi, con investimenti efficaci ed adatti ai rischi aziendali per essere preparati ad affrontare il sinistro e i costi/danni che ne derivano. Le Assicurazioni servono a trasformare un costo/danno incerto e spesso insostenibile in un costo/premio programmato e sostenibile. La scelta merita una attenta valutazione in fase di prevenzione, affinché effettivamente funzionino da paracadute finanziario

ed economico e ci permettano di restare sul mercato evitando la chiusura,perdite bilancio non recuperabilie fornendo gli strumenti per salvaguardare la reputazione del brand.

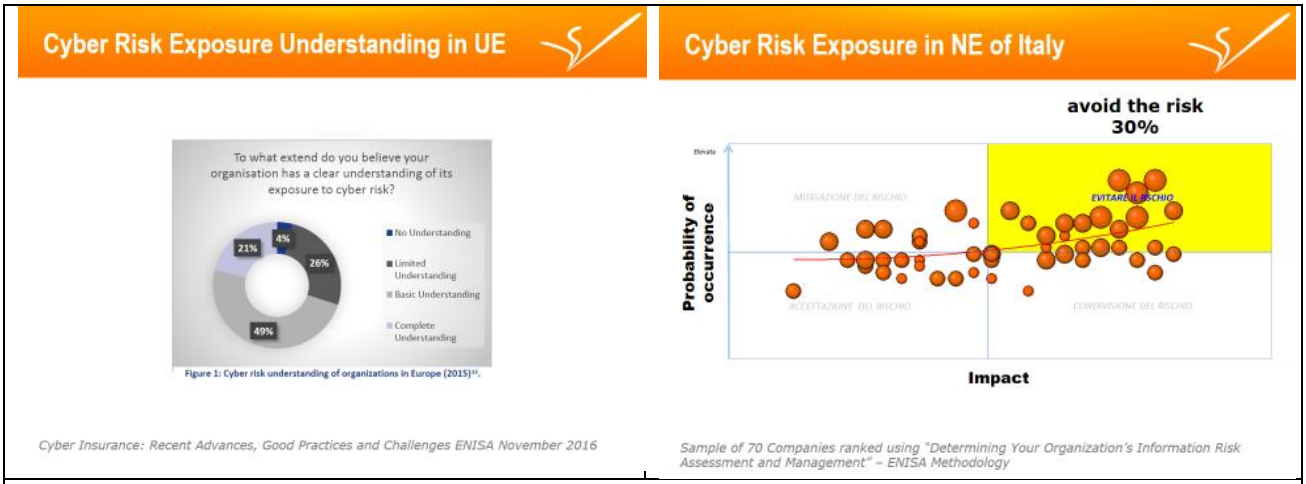


Fonte: Chubb Claim Trends 8/2016

Cyber Risk Exposure e Cyber Risk Insurance

Parlare di Cyber Risk Insurance, ovvero una polizza o un insieme di polizze atte a "coprire" i danni e costi derivati da un incidente cyber o cyber-correlato, non ha senso se non c'è consapevolezza della propria esposizione al rischio e non si prendono misure di mitigazione della "reale" esposizione.

I risultati della survey sull'esposizione al rischio



Fonte: Presentazione Whitepaper Cyber Risk Exposure & Insurance – Infosek 2016 - Slovenia

La ricerca sull'esposizione al rischio svolta da Via Virtuosa nell'arco di 3 anni e confluita nel Whitepaper, "evidenzia non tanto il posizionamento della singola azienda e la sua esposizione al rischio, bensì

l'andamento statistico del campione intervistato, nella fattispecie appartenente al territorio del Nord-Est,rispetto a una *Base Line* di riferimento (Linea Rossa). La metodologia di misurazione usata è oggettiva (come per la 2700x) ed uguale per tutto il campione, anche se notevolmente semplificata. Si tratta di quella adottata da European Union Agency for Network and Information Security (ENISA).

Chi rientra nel quadrante in alto a destra (giallo) ha una esposizione al rischio significativa e con un impatto potenzialmente *disruptive*sul business. Chi si trova in questo quadrante viene invitato (in base alla stessa metodologia) ad "esternalizzare il rischio."

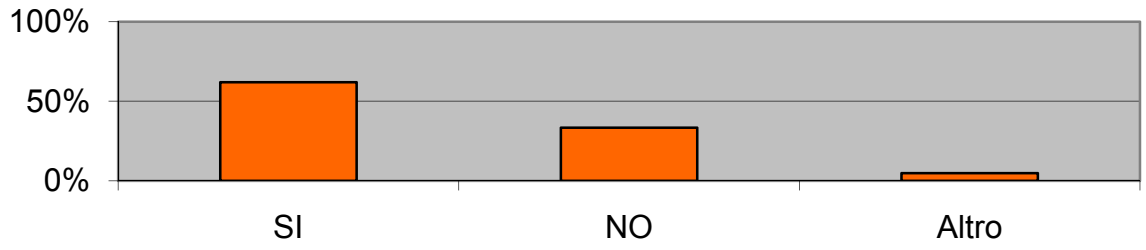
Questa ricerca ha fatto emergere i seguenti aspetti:

- Esiste un elevato rischio Cyber per le aziende che impatta direttamente sulla continuità del businness
- C'è consapevolezza del reparto IT sul problema, ma mancanza pressoché totale di sensibilità da parte del board aziendale che si traduce in scarsi investimenti
- Manca una misurazione oggettiva del rischio Cyber da parte delle aziende
- Emergono indicazioni oggettive per il trasferimento del rischio Cyber all'esterno dell'azienda.

I risultati della survey su CIO e Cyber Risk Insurance

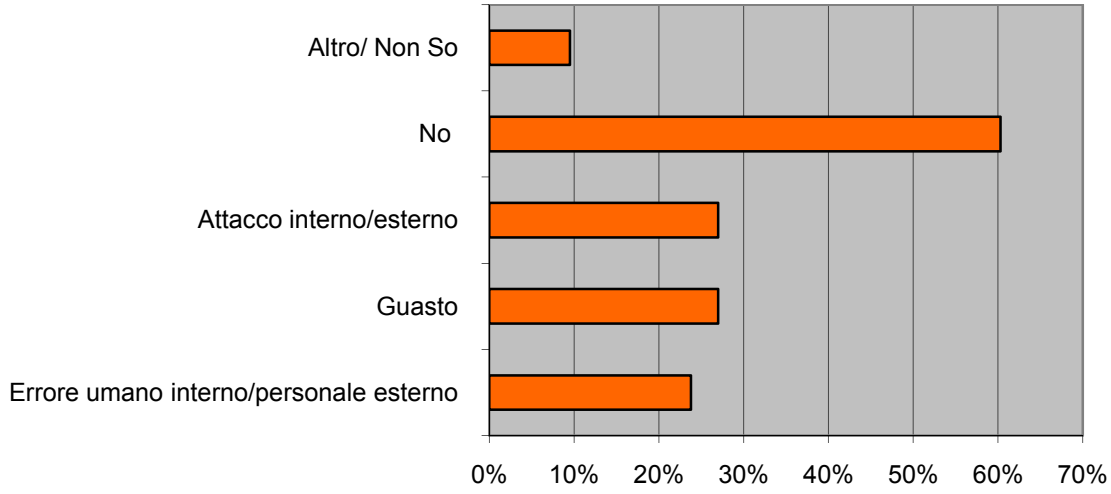
Il campione di questa seconda indagine vede prevalere il settore industria e servizi (rispettivamente il 40% e 35%) con fatturato sopra i 20 Mln Euro (75%) e con più di 100 addetti (50% tra 100-500 e 30%> di 500).
Questo ci fa presumere che aspetti come la **Reputazione**, il**Fermo d'Attività** e la gestione dei **Dati Sensibili** possano essere aspetti critici.
La survey ha richiesto in prima istanza agli IT Manager, quale sia, allo stato dell'arte, 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).

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



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

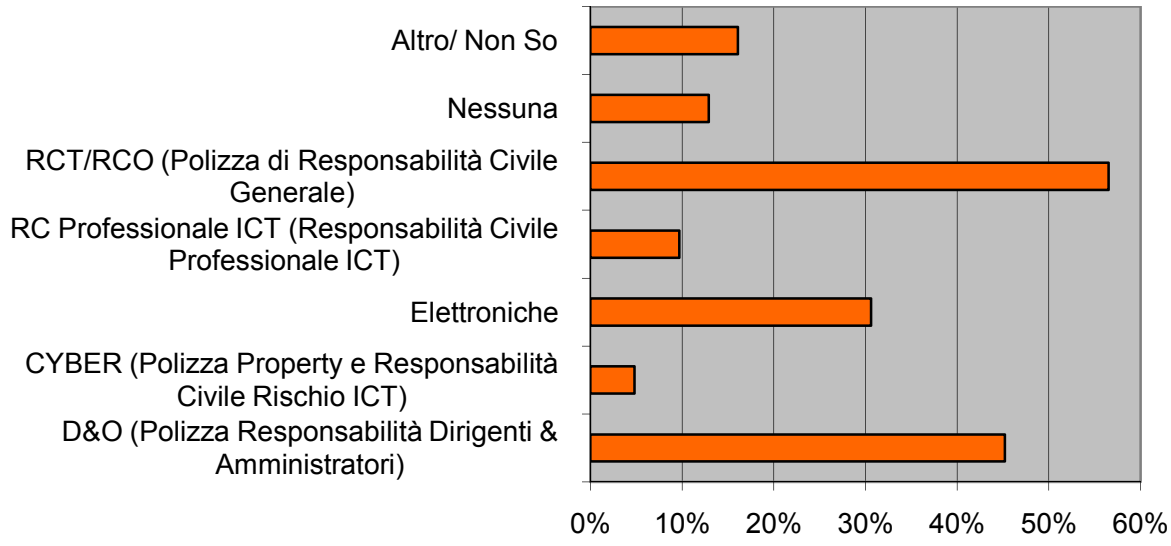
DOMANDA 4: Le hanno mai chiesto di evidenziare i costi/danni che presume possano derivare da un sinistro cyber? (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Quindi è stato chiesto loro di compiere quello che probabilmente è un passo insolito: interfacciarsi con il collega CFO per poter rispondere al quesito sulla presenza o meno in azienda di alcune polizzeche dovrebbero essere prese in esame rispetto ai punti critici emersi nell'analisi sull'esposizione al rischio.(quesito 3)

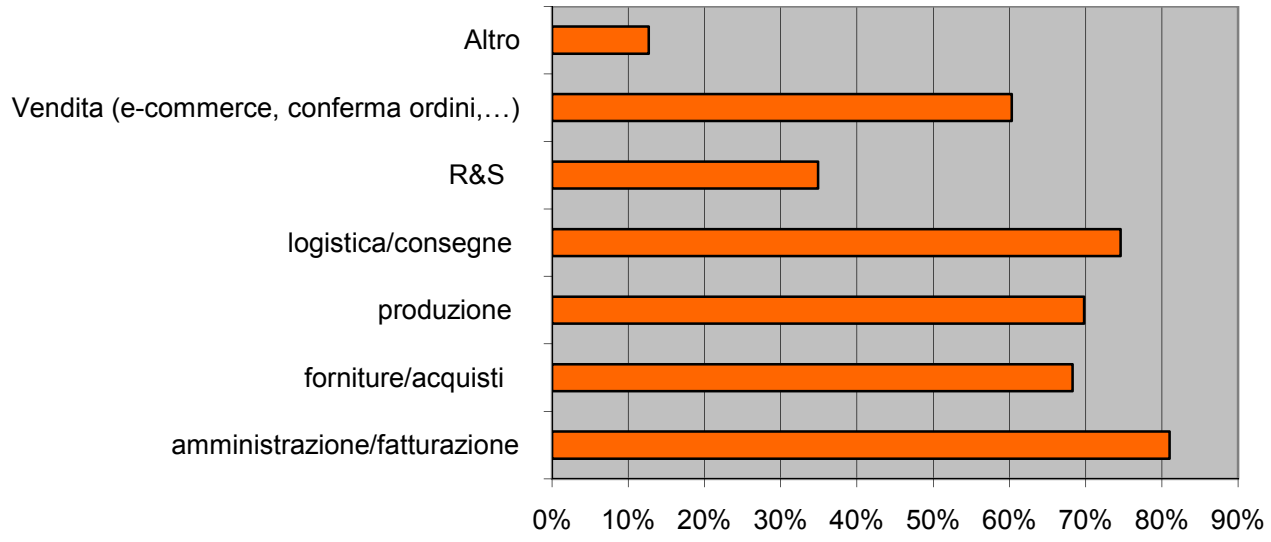
DOMANDA 3: Esistono in azienda queste polizze? (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Un 60% dei CIO viene coinvolto in un approccio ampio di security. Sempre 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 potrebbero soffrire di più di una interruzione d'attività (quesito 8).

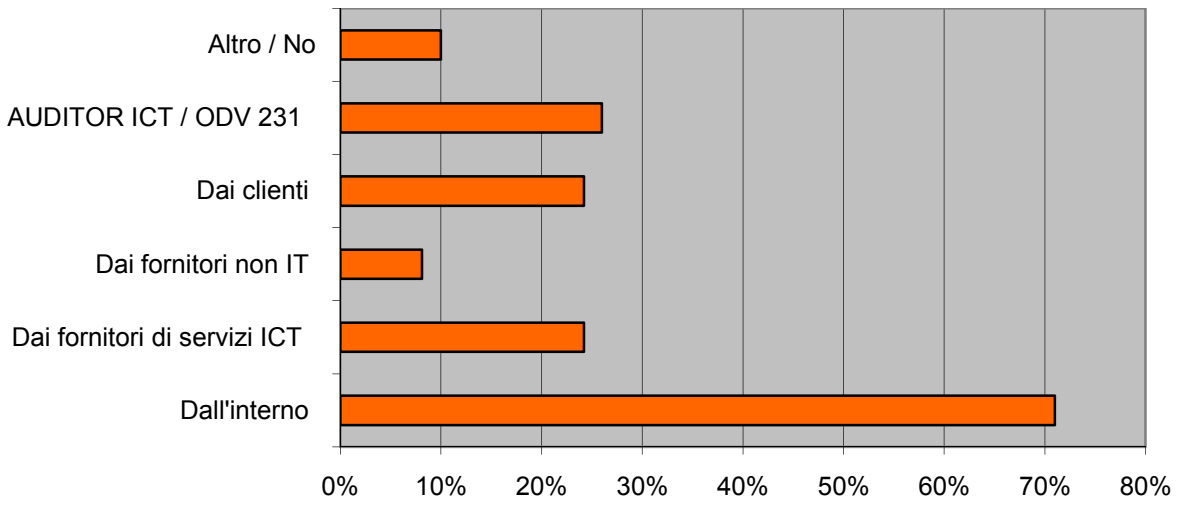
DOMANDA 8: Un fermo di attività ICT su quali aree di lavoro aziendale può impattare (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Il CIO si occupa di sicurezza informatica: attua un controllo delle vulnerabilità (60% dei casi) e piani di Business Continuity e Disaster Recovery (50-60% dei casi), invece molto poco di crisi reputazionale (18%), di formalizzare delle procedure/policy (28%) o modellizzare le problematiche (12%).
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%). Quest'ultimo dato potrebbe crescere in futuro e condurre ad un controllo della filiera in termini di virtuosità della gestione e dunque anche dell'assicurazione e comunque essere una buona premessa per strutturare un percorso di Cyber Risk Management.

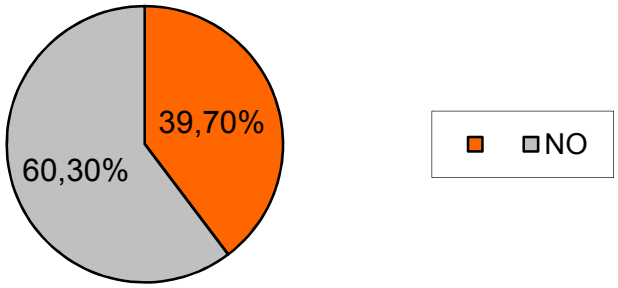
DOMANDA 7: All'ICT manager sono pervenute richieste in merito alla gestione della sicurezza ICT? (Anche più di una risposta)



Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Il 39% dichiara di essere a conoscenza di sinistri avvenuti negli ultimi 5 anni. Andando a vedere i dettagli del tipo di cause, sostanzialmente esse sono riconducibili in misura pressoché equa all'attacco (esterno/interno) con una prevalenza di Ransomware, all'errore umano (interno/esterno) e al guasto(q. 9).

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.

Fonte: Whitepaper "Cyber Risk Exposure & Cyber Risk Insurance", Via Virtuosa 12/2016

Quanto emerso dal quesito 8 sullavisione del CIO riguardo agli impatti più pesanti di un fermo di attività ICT su Amministrazione/fatturazione (+ 80%), logistica e consegne (73%) e vendite (60%) ci permette di tornare al valore e alla funzione dell'outsourcing assicurativo:Mancati pagamenti ai fornitori, mancati ordini o mancate consegne possono incontrovertibilmente causare problemi al bilancio nel breve, medio o lungo periodo.
Le aziende "virtuose", ovvero che hanno attivato percorsi di Cyber Risk Management, potranno quindi presentarsi al tavolo assicurativo consapevoli del **rischio residuo da** trasferiresoprattutto per il**fermo d'attività, problematiche cyber dolose/accidentali** e **responsabilità civile generale o professionale,** valutando correttamente, ove fosse necessario, anche il **rischio reputazionale**.

Con il CIO al tavolo del Cyber Risk Management

I risultati dell'indagine ci permettono di dire che il CIO possa essere il "mediatore culturale" in azienda, coadiuvato da un competente interlocutore assicurativo.

Riepiloghiamo qui in modo sintetico le attività di un ipoteticotavolo operativo per la gestione del rischio cyber:

Cyber Risk Exposure e proattività: sapere quanto e come siamo esposti

- ✓ qualificare e quantificare gli asset e il loro valore
- ✓ qualificare l'esposizione e il valore dell'esposizione ovvero le conseguenze operative e finanziarie di un sinistro
- ✓ qualificare e quantificare investimenti in mitigazione
- ✓ verificare le coperture assicurative interne e dei propri fornitori

Ora si hanno gli strumenti e le conoscenze per affrontare un discorso assicurativo e TRASFERIRE IL RISCHIO RESIDUO.

Cyber Risk Insurance: trasferire il rischio residuo alle Assicurazioni

- ✓ Individuare un partner assicurativo preparatoe analizzare la posizione assicurativa aziendale
- ✓ Verificare le **polizze tradizionali presenti in azienda** con cui mettere in relazione la copertura cyber
- ✓ Scegliere e strutturare una assicurazione Cyber che affronti in maniera specifica i rischi da trasferire e relativi costi (interruzione di esercizio, responsabilità generale e professionale, violazione o uso improprio degli assets, difesa della reputazione, contromisure di reazione ed analisi, etc.)

Per il dettaglio si rimanda al Focus On Report Clusit 2016.

Cosa è emerso dal "dialogo" tra CIO e Assicuratore – Risposte sulla Cyber Risk Insurance

Abbiamo chiesto a tre CIO di rilevanti realtà aziendali del Nord-Est, di porre in libertà le domande che potessero far comprendere a un non addetto ai lavori opportunità e limiti dello strumento assicurativo. Ecco un sintesi delle risposte ad alcune delle domande più ricorrenti (18) emerse da questo confronto:

C'è la la necessità di **esaminare le polizze esistenti** e verificare la loro aderenza alle problematiche ICT emerse in fase di analisi;

Ad oggi non è richiesto uno standard condiviso per la misurazione dell'esposizione.**Eventuali best practice, certificazioni** volte a mitigare il rischio possono **favorire il processo di trasferimento del rischio** all'assicurazione con accesso a migliori condizioni di copertura;

GDPR e Assicurazione: sarà molto importante sapere se si detengono Dati Sensibili secondo la definizione ampliata prevista dal nuovo Regolamento, in quale paese e quali misure si prendono per difendersi dal *data breach*. Se si affidano i Dati Sensibili propri o quelli di Terzi a noi affidati a un terzo soggetto, vanno analizzati i contratti in essere con questo fornitore e le eventuali manleve presenti, per poter trasferire in maniera corretta i costi derivanti dagli obblighi presenti nel GDPR. Se si **scrive o personalizza codice,** si dovrà valutare molto bene l'ambito della propria responsabilità (professionale, generale, di prodotto);

Simulare l'impatto di un evento Cyber sul bilancio aziendale, in termini di aumento costi e perdita di profitto lordo. E' forse il campo più critico e sottovalutato, ma ben noto agli assicuratori sotto il nome di Businness Interruption.

In conclusione, emerge con chiarezza che il percorso di Cyber Risk Management, deve passare attraverso una stretta collaborazione dei risk owner aziendali col CIO e il CFO, la costruzione di una filiera virtuosa che comprenda clienti e fornitori, l'aiuto di **professionisti IT preparati nella gestione ed implementazione** della Cyber Security ed **intermediari esperti in materia cyber** in grado di supportare l'Azienda nella scelta del giusto equilibrio tra costo e garanzie assicurative.