LE INTERVISTE DI NEXTVALUE

CYBERSECURITY: I CFO RISPONDONO

Fornitori, assicurazioni, budget e policy nelle strategie di Cybersecurity

NEXTVALUE
INSIGHTS FOR YOUR BUSINESS

Si ringrazia:
Dott. Roberto Mannozzi
Direttore Centrale Amministrazione, Bilancio e Fiscale del Gruppo FS Italiane
Presidente

ANDAF
Associazione Nazionale
Direttori Amministrativi e Finanziari

A cura di:

Martina Longo
Research Manager @NEXTVALUE

Manuela Moroncini
Content Manager @NEXTVALUE

In collaborazione con:
CITRIX®

Sommario

Introduzione

Gestire i rischi connessi al mondo Cyber è senz'altro molto più difficile che in passato. L'uso pervasivo e crescente di tecnologie e strumenti abilitanti la trasformazione digitale ha virtualmente impatto su ogni aspetto del business, dalla reputazione al bilancio aziendale, ed il Rischio Cyber non è più solo un problema del Dipartimento IT ma richiede una strategia di management condivisa dal Board e dalla prima linea aziendale.

Tuttavia, in molti casi l'organizzazione interna delle imprese riflette ancora una tradizionale divisione "a silos" tra le diverse Figure, le quali si interfacciano con interlocutori differenti e tra cui mancano occasioni di dialogo attivo, ponendo di fatto un freno all'innovazione tecnologica, ed un ulteriore rischio per la sicurezza delle informazioni aziendali.

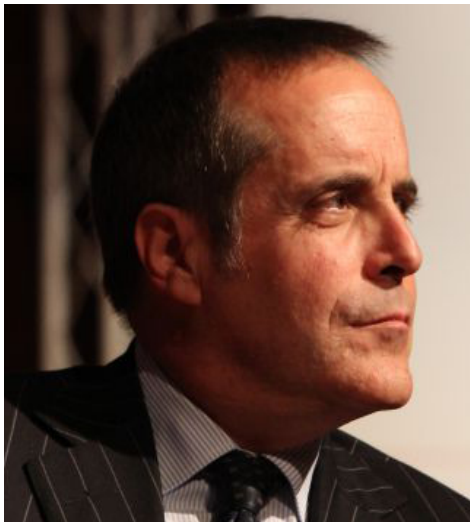
In questa direzione, NEXTVALUE ha avviato un progetto innovativo che prevede la realizzazione di una collana di interviste esclusive su Industria 4.0 e Cybersecurity, con autorevoli professionisti, leader nei rispettivi ambiti – legale, fiscale, accademico - dedicata ai Decisori IT, ai Responsabili della Cybersecurity e ai CIO delle aziende end-user.

Obiettivo di ogni intervista è condividere una check-list preparata dai Decisori non-IT per i Decisori IT.

In questa intervista approfondiamo gli aspetti di gestione del rischio legato alla Cybersecurity dal punto di vista dei CFO e Direttori Amministrativi. Cogliamo l'occasione per ringraziare Roberto Mannozzi, Presidente di ANDAF e Direttore Centrale Amministrazione, Bilancio e Fiscale del Gruppo FS Italiane per il prezioso contributo di pensiero fornito e per il tempo che ci ha dedicato.

Le altre interviste sono disponibili su www.nextvalue.it alla sezione Interviste.

L'esperto



Dott. Roberto Mannozzi

Direttore Centrale Amministrazione,
Bilancio e Fiscale del Gruppo FS Italiane
Dirigente Preposto alla redazione dei documenti contabili societari

Presidente

ANDAF
Associazione Nazionale
Direttori Amministrativi e Finanziari

Roberto Mannozzi è Direttore Centrale Amministrazione, Bilancio e Fiscale del Gruppo FS Italiane, alle dirette dipendenze dell'Amministratore Delegato, e Dirigente Preposto alla redazione dei documenti contabili societari.

Ha ricoperto, e ricopre tuttora, diversi incarichi sia di Amministratore che di Sindaco revisore in varie società ed organismi, interni ed esterni al Gruppo FS, fra i quali spiccano quello di Amministratore in Netinera Deutschland GmbH, capogruppo tedesca controllata da FS S.p.A. che comprende circa 40 subsidiaries di trasporto locale su ferro in Germania, quello di membro del Consiglio di Sorveglianza dell'OIC, l'Organismo Italiano di Contabilità che svolge il ruolo di national standard setter in materia di principi contabili ai sensi della legge n. 116/2014, e quello di Presidente del CdA di Centostazioni SpA, anch'essa controllata da FS S.p.A.

E' Presidente di ANDAF, l'Associazione Nazionale Direttori Amministrativi e Finanziari, con oltre 1.600 soci rappresentati principalmente dai CFO di società e gruppi italiani.

01

Che ruolo ha il Chief Financial Officer nella predisposizione di misure di Cybersecurity in sede preventiva, rispetto ad un potenziale attacco informatico? E in sede di rimedio, nell'ipotesi di un attacco già avvenuto?

Roberto Mannozzi (FS Italiane): La Cybersecurity è sicuramente un tema di rilevanza assoluta anche perchè il crimine cyber presenta un bassissimo rischio rispetto ad altre attività illegali, ed è favorito dalla rapidità di evoluzione delle minacce.

Molte aziende subiscono attacchi cyber senza esserne consapevoli. Un attacco cyber può danneggiare non solo le operations ma anche e soprattutto l'immagine dell'azienda, avendo importanti ricadute sui "numeri" di bilancio, come dimostrano i tanti attacchi avvenuti negli ultimi anni.

La rilevanza e la consapevolezza di tali rischi da parte dei CFO è confermata dalla survey "I sistemi amministrativo contabili a supporto dei CFO" condotta da ANDAF sui CFO di alcuni tra i più importanti gruppi italiani. Dai risultati della ricerca è emerso come il rischio cyber ed in generale il rischio informatico sia a tutti gli effetti un rischio d'impresa e, conseguentemente, il piano strategico di sicurezza informatica debba diventare parte integrante della strategia aziendale.

In materia di prevenzione dei rischi Cyber ritengo sia fondamentale operare su più fronti, contemporaneamente:

- Definire una strategia di cooperazione tra le Aziende, le Organizzazioni pubbliche e le Istituzioni (vedi anche il DPCM sulla Cybersecurity del 17 febbraio 2017).
- Costruire un solido Sistema di Controllo Interno, dato che l'errore umano e il dolo sono tra le cause più significative dei rischi cyber occorsi alle imprese.
- Diffondere le policy sulla gestione delle informazioni sensibili ai dipendenti, spesso rei di non esserne a conoscenza. In tale ottica, l'adozione strutturata del regolamento generale sulla protezione dei dati GDPR, a partire dal 28 maggio 2018, è un efficace strumento di prevenzione.
- Adottare e diffondere in azienda la cultura del Risk Management, per far comprendere alle figure apicali dell'azienda l'importanza della gestione del rischio in tutti i suoi aspetti e definire, in maniera strutturata, come gestire, mitigare o eventualmente trasferire all'esterno il rischio stesso.

In sede di rimedio, ritengo importante adottare una gestione collaborativa delle crisi cyber, come tra l'altro indicato dal già citato DPCM, attivando una comunicazione strutturata con le Istituzioni.

La sicurezza deve comprendere la valutazione dei fornitori? Esistono ambiti da monitare con particolare attenzione? Che cosa non dovrebbe sottovalutare il Responsabile della Sicurezza o un Direttore IT, nella scelta di un fornitore?

Roberto Mannozzi (FS Italiane): Con il diffondersi delle nuove tecnologie ed i servizi Cloud based, il tema della Sicurezza IT ed in particolare la scelta del fornitore diventano di fondamentale importanza.

Ritengo sia molto importante che si instauri ed alimenti un dialogo attivo tra le diverse Funzioni aziendali, in particolare tra coloro che si occupano di IT, di Sicurezza aziendale, di Risk Management, di Procurement, e l'ufficio legale, con l'obiettivo di definire i requisiti minimi e le condizioni contrattuali accettabili per l'azienda.

Il punto è di estrema attualità e merita la massima attenzione da parte delle grandi aziende che inconsapevolmente assumono rischi importanti, laddove gli attacchi ai loro sistemi avvengono spesso sfruttando le "debolezze" nelle piccole e meno strutturate aziende fornitrici.

Mi riferisco a quei fornitori, spesso liberi professionisti o studi associati, come ad esempio gli studi legali, che sono in possesso di informazioni sensibili delle nostre aziende, e che non sempre dispongono dei sistemi di sicurezza IT adeguati.

Nell'interesse delle nostre aziende, credo sia assolutamente vitale ricercare e alimentare costantemente una stretta cooperazione tra le diverse funzioni aziendali, per arrivare a definire i requisiti IT minimi, da far rispettare a tutti i fornitori e opportunamente da esplicitare all'interno delle condizioni contrattuali di fornitura.

03

L'assicurazione sul Cyber Risk è già o sarà una soluzione? Che ruolo ha il Chief Information Officer (CIO) e/o il Responsabile della Sicurezza (CSO/CISO) nella sottoscrizione di un contratto di assicurazione Cyber? E nella sua gestione?

Roberto Mannozzi (FS Italiane): Data l'asimmetricità e la pervasività della minaccia cyber, non esiste oggi la possibilità di proteggersi completamente contro i Rischi Cyber. Il mercato assicurativo italiano è in rapida evoluzione, ma l'offerta di polizze Cyber risk è ancora in fase embrionale.

Un solido Risk Management, rende però le aziende consapevoli dei propri rischi e costituisce la base di partenza per una loro corretta gestione. Una gestione consapevole del Rischio Cyber, di fatto poi integra le strategie di prevenzione, di mitigazione e di ottimizzazione e crea le condizioni per il trasferimento consapevole del rischio sul mercato assicurativo.

Il processo di analisi e valutazione del rischio è sempre preventivo e propedeutico alla possibilità di attivare una cd. Cyber Insurance. In presenza di business particolarmente complessi, una copertura assicurativa contro il Cyber Rischio può diventare un elemento di difesa importante, e soprattutto utile, di tutela del bilancio aziendale, contro i cosiddetti "rischi catastrofali", anch'essi variabili in funzione del livello di tolleranza al rischio di ciascuna impresa.

L'analisi dei rischi collegati ad un attacco Cyber risulta peraltro particolarmente complessa. Se da una lato, il rischio di perdite derivanti da un attacco informatico è quantificabile in base ai tempi di mancata operatività, dall'altro è molto più complesso valutare l'entità dei danni immateriali subiti a fronte di un attacco Cyber, come ad esempio quello reputazionale. A questo si aggiunga che la quantificazione dei danni immateriali trova comunque un limite superiore, rappresentato dal massimale, preventivamente condiviso e accettato dalle società di assicurazioni.

Per alcuni Responsabili della Sicurezza di grandi imprese, intervistati da NEXTVALUE, il budget a disposizione è meno "critico" rispetto alla definizione del corretto mix di investimenti in soluzioni e servizi contro i Rischi Cyber. Qual è il suo parere?

Roberto Mannozzi (FS Italiane): A mio avviso sono vere entrambe le indicazioni.

Da un lato, la disponibilità ad investire in sicurezza continua ad essere bassa, almeno fino a quando non si subisce seriamente un attacco Cyber, in funzione del quale l'impresa acquisisce la consapevolezza del rischio e diventa "disponibile" ad investire.

Dall'altro, vi è la difficoltà oggettiva di identificare le soluzioni software ed i servizi su cui investire per prevenire e gestire tali tipologie di rischio, anche in considerazione della rapida evoluzione delle tecnologie e di conseguenza dei rischi informatici.

A mio parere, ritengo sia importante collaborare con le Istituzioni e analizzare le best practice in materia, al fine di definire il giusto mix di investimenti.

Oltre ai necessari investimenti in tecnologia, poi diventa di fondamentale importanza investire nella strutturazione di metodologie di analisi e valutazione dei rischi, che una volta impostate non possono prescindere dal monitoraggio continuo degli scenari di minaccia.

05

10

Troppe policy possono portare minore sicurezza. Esiste un mix ideale tra la "spesa in software e tecnologie" e la "spesa in formazione dei collaboratori" che sia idoneo a diffondere una cultura della sicurezza a tutti i livelli gerarchici dell'azienda?

Roberto Mannozzi (FS Italiane): Come ormai è noto, la maggior parte degli attacchi proviene dall'interno delle aziende. Spesso le informazioni sensibili vengono gestite dai dipendenti senza che questi abbiamo la piena consapevolezza dei rischi che i loro comportamenti errati potrebbero causare alle loro aziende.

In quasi tutte le organizzazioni di grandi dimensioni, esistono elaborate policy e procedure sulla gestione delle informazioni, dei file e delle e-mail contenenti informazioni sensibili. A mio parere, in tutte queste realtà, esiste un problema concreto rappresentato dal fatto che tali procedure non sempre sono conosciute dai dipendenti o se lo sono, vengono applicate poco.

Ritengo quindi di primaria importanza investire in change management e in formazione, anche e soprattutto in tempi come questi in cui è sempre più frequente l'utilizzo e l'accesso in mobilità ai dati aziendali. Mentre in passato i dipendenti utilizzavano solo gli "strumenti di lavoro", pc portatile, smartphone ecc. che le aziende mettevano loro a disposizione, negli ultimi anni si è accresciuta la tendenza ad utilizzare i propri dispositivi personali anche per lavorare, dando origine ad ulteriori rischi.

NEXTVALUE

Azienda indipendente di ricerca di mercato B2B, sui temi emergenti dell'Information Technology fondata da Alfredo Gatti nel 2003.

I nostri interlocutori per l'attività di ricerca sono i Decisori IT delle aziende end-user. I nostri Clienti i principali player del sistema di Offerta IT. Essi ci riconoscono una posizione privilegiata e ci attribuiscono un ruolo di collegamento tra Domanda e Offerta IT.

Autori di programmi e contenuti originali, abbiamo curato per 11 anni l'Assintel Report, la Ricerca sulla Domanda IT in Italia, su incarico di Assintel e Confcommercio e nel 2017 la sezione "La trasformazione digitale vista dai CIO" del rapporto "Il digitale in Italia 2017", su incarico di Assinform e Confindustria digitale.

NEXTVALUE ha fondato nel 2010 il chapter italiano di CIONET, la prima business community di CIO e Direttori IT di aziende Top e Medio Grandi in Europa e America Latina.

NEXTVALUE
INSIGHTS FOR YOUR BUSINESS

Strada della Carità 8, 20135 Milano
tel 02 8976 3767
info@nextvalue.it
www.nextvalue.it