aiceo
Associazione Italiana

LE INTERVISTE DI NEXTVALUE

CYBERSECURITY
I CEO RISPONDONO

RICCARDO BELLINI
COUNTRY MANAGER ITALIA
VALEUR ASSET MANAGEMENT

NEXTVALUE
INSIGHTS FOR YOUR BUSINESS

A cura di:

Manuela Moroncini
Content Manager @NEXTVALUE

Maggio 2018

Sommario

Introduzione

Con la diffusione e la pervasività delle tecnologie all'interno delle strutture organizzative e la crescente attenzione mediatica riservata agli effetti prodotti dagli attacchi informatici, le iniziative di Cybersecurity vedono i Chief Executive Officer e gli Amministratori Delegati sempre più direttamente coinvolti, come principali stakeholder nella loro gestione.

Se gli attacchi informatici sono a volte più rapidi a cambiare dell'innovazione stessa, la Cybersecurity diventa un elemento imprescindibile di salvaguardia di un perimetro aziendale sempre più esteso e fluido, dove le maggiori criticità derivano dai dispositivi mobili consumer - smartphone e tablet in dotazione alle risorse umane - e in prospettiva da tutti i dispositivi connessi in ottica M2M.

Il crimine informatico continuerà ad evolvere e ad adattarsi alle nuove misure di sicurezza. C'è chi ipotizza che il Cybercrime stia per esplodere come una vera e propria industry. La minaccia complessiva si tradurrà in maggiori spese per le aziende, non solo per le violazioni subite e per il lavoro di prevenzione, ma per i maggiori danni che potrebbero derivare all'immagine aziendale e conseguentemente alle capitalizzazioni di borsa.

Il problema principale per i CEO e gli Amministratori Delegati non è più quale software acquistare e da chi, ma quale cultura diffondere. La cultura diventa la chiave di volta nella lotta al Cybercrime. In NEXTVALUE crediamo fermamente nell'innovazione dei modelli di business e il nostro obiettivo è contribuire allo sviluppo di una cultura dell'automazione in tutte le aziende.

Siamo orgogliosi di avviare un ciclo di interviste esclusive sui temi dell'innovazione a cui hanno preso parte i più autorevoli opinion leader e Capitani d'impresa del nostro Paese. Il risultato è ricco di spunti e riflessioni che con estremo piacere condividiamo con una platea ampia e qualificata di Direttori IT delle principali organizzazioni italiane.

In questa intervista approfondiamo aspetti singolari sulla Cybersecurity, sul suo ruolo come leva di innovazione, sulle nuove minacce, sulle strategie di difesa, e sul crescente ruolo assunto dalle compagnie di assicurazione.

Cogliamo l'occasione per ringraziare Riccardo Bellini, Country Manager Italia di Valeur Asset Management per il prezioso contributo di pensiero fornito e per il tempo che ci ha dedicato e AICEO, Associazione Italiana CEO, per l'incoraggiamento e la fiducia accordataci nella realizzazione di questo ciclo di interviste, con i CEO suoi membri, su temi come Cybersecurity, Intelligenza Artificiale e Industria 4.0.

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

Buona lettura!

Il CEO

Riccardo Bellini

Country Manager Italia
Valeur Asset Management

Riccardo Bellini, Country Manager Italia, entra in Valeur Asset Management a Gennaio 2017 dopo una esperienza di sette anni nel Gruppo Azimut.

Nella prima parte della sua carriera professionale ha lavorato presso la compagnia di assicurazioni AXA MPS a Dublino occupandosi di sviluppo prodotti e distribuzione sul mercato italiano.

Successivamente entra nella direzione commerciale del Gruppo Azimut, con il ruolo di Network Training and Development Officer di tutto il Gruppo. Nel corso degli anni ha coordinato direttamente parte della rete dei consulenti finanziari e ha ricoperto anche il ruolo di Responsabile dei prodotti e servizi di Wealth Management.

Riccardo si è laureato in giurisprudenza all'Università Statale di Milano, ha conseguito un master in Assicurazioni e Previdenza presso la LIUC Università di Castellanza, ha conseguito il diploma per il corso di specializzazione "Wealth Management Executive Program" presso la SDA Bocconi School of Management e infine è iscritto all'albo dei consulenti finanziari.

01

Qual è la difficoltà maggiore che vede oggi nel rendere la sicurezza una effettiva leva di business, al di là della compliance e dei regolamenti europei che entreranno presto in vigore?

Riccardo Bellini: Nel settore degli investimenti finanziari la protezione dei dati e la sicurezza informatica ha sempre rivestito una grande rilevanza proprio per la mole di informazioni personali e patrimoniali che vengono trattate ogni qual volta un investitore (sia esso privato, famiglia o azienda) decide di affidarsi a un intermediario finanziario. Qualsiasi società sia essa una SIM, una SGR, una Banca, una Family office, una Fiduciaria o un'impresa di Assicurazioni, per poter aprire una relazione con il cliente deve possedere copia della carta di identità e del codice fiscale, deve profilarlo e quindi conoscere il lavoro che svolge, il reddito percepito, l'entità del patrimonio complessivo e la composizione dello stesso, i nomi dei famigliari e altro ancora. Informazioni che devono essere assolutamente protette e gestite con professionalità ed estrema attenzione.

In un mondo complesso e articolato come quello in cui viviamo, le imprese non devono solamente occuparsi di innovazione, ricercando nuove soluzioni di investimento, nuove forme di comunicazione, nuovi canali di business ma anche predisporre sistemi, processi e funzioni aziendali che tutelino i dati sensibili della propria clientela. Questo aspetto, se ben gestito, contribuirà a rafforzare la fiducia degli investitori e a fortificare la reputazione dell'azienda; aspetti che, inevitabilmente, concorreranno anche allo sviluppo del business.

Al di là dell'entrata in vigore del regolamento europeo sulla protezione dei dati personali (GDPR), è necessario che le aziende rivedano fin da subito i propri processi interni ponendo la sicurezza degli utenti/clienti o investitori, come elemento primario a cui assegnare la massima priorità.

L'ostacolo che rende oggi la sicurezza una vera leva di business è, ad oggi, l'effettiva percezione della sua importanza attribuita da ogni singolo operatore del settore e dai suoi dipendenti. Da recenti analisi di mercato è emerso che, per i risparmiatori, il fattore fiducia è uno degli elementi fondamentali nella scelta della banca o della società di investimento a cui decidono di affidarsi. Per questo motivo la sicurezza e la riservatezza dei dati personali assumono un ruolo di assoluta importanza.

Come è variata la sensibilità dei suoi clienti rispetto al tema della sicurezza dei dati personali? Il rischio Cyber è effettivamente un rischio strategico e di business o continua ad essere un problema riservato agli esperti di informatica?

Riccardo Bellini: La sicurezza dei dati personali sta diventando un tema cruciale non solo per le aziende ma anche per i clienti. Personalmente ritengo che la tutela dei dati personali sia in primis una forma di rispetto nei confronti dei clienti oltre che una normativa da rispettare.

I recenti fatti, uno su tutti il caso Cambridge Analytica, hanno alzato il livello di allerta generale, modificando notevolmente la percezione di rischio relativo alla sicurezza dei propri dati "sensibili".

Ogni organizzazione non dovrebbe limitarsi a prendere in considerazione e, di conseguenza, tutelarsi solo dai Rischi Cyber, ma è opportuno che gestisca con attenzione anche i luoghi fisici di lavoro. Servono procedure e strutture adeguate, come ad esempio armadi/archivi dotati di chiavi e un dispositivo tritacarte, ma soprattutto personale di fiducia, attento e formato. Avere un sistema informatico sicuro è fondamentale, ma non è sufficiente se poi i contratti contenenti le informazioni sul patrimonio dei clienti sono accessibili a estranei, quali ad esempio l'impresa di pulizia che ha accesso agli uffici al termine dell'orario di lavoro.

La GDPR arriva in un momento cruciale e porterà non pochi cambiamenti, come ad esempio l'inserimento in azienda di una funzione specifica che si occuperà di analizzare e controllare i rischi per evitare ingenti sanzioni in caso di violazione della normativa.

Inoltre, l'utilizzo dei social network e degli smartphone che negli ultimi anni è cresciuto esponenzialmente, non solo tra le nuove generazioni, che faticano a vivere senza "condividere" e "postare" ogni momento della propria vita, ma anche tra le fasce di età più alte, impone la massima attenzione sugli impatti e sulle ripercussioni che un utilizzo superficiale di questi nuovi canali di comunicazione possono avere sulla tutela delle nostre informazioni sensibili. Recepire una normativa severa, che tutela la sicurezza dei dati sensibili, è fondamentale per contrastare i rischi a cui tutti noi siamo esposti.

03

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 aziendali?

Riccardo Bellini: Tecnologia, procedure e formazione sono il giusto asset mix per affrontare le sfide che ci sottoporrà la GDPR. Affermare che è più importante investire in tecnologia piuttosto che in formazione, o viceversa, è sbagliato se prima non viene fatta una valutazione aziendale sull’impatto della protezione dei dati. Solamente dopo avere chiara la visione d’insieme, si sarà in grado di stabilire e pianificare le misure di protezione più adatte e la loro priorità (aggiornare o implementare le applicazioni informatiche di supporto, predisporre processi aziendali, ideare un percorso formativo per i dipendenti, etc.).

La normativa lascia però alle singole organizzazioni, secondo il principio dell’Accountability, la responsabilità di scegliere gli strumenti più idonei a raggiungere lo scopo. La scelta se investire più in software o formazione dipende pertanto dal modello di business e da come è strutturata l’azienda stessa, dalla qualità dei sistemi informatici, dai livelli di protezione contro gli attacchi informatici, da come vengono archiviati i dati, da chi vi ha accesso, e non da ultimo dal livello di sensibilità e cultura che è stato trasmesso a tutto il personale dell’azienda.

Così su due piedi se una azienda affrontasse il tema da zero, la priorità dovrebbe essere data all’implementazione di software e strumenti tecnologici adatti a proteggere la struttura da attacchi esterni e a controllare che non vi sia dispersione di dati dall’interno. Attività che richiede significativi investimenti di denaro ma anche l’impiego di persone qualificate che sappiano individuare i controlli essenziali e stimare costantemente la loro implementazione. Solo in un secondo momento, la formazione entrerebbe in gioco per creare una sana cultura aziendale sul tema e istruire il personale su come comportarsi di fronte a situazioni che spaziano dal virus preso sul proprio pc, alla perdita di un device (quale per esempio lo smartphone), alla tutela delle proprie user e password, fino alla gestione di tutti i documenti cartacei che vengono generati dalle stampanti che tutti gli uffici possiedono e che non hanno misure di sicurezza.

Cosa dobbiamo attenderci dal Cybersecurity Tech Accord, l'accordo firmato il 17 aprile 2018 con l'obiettivo di alzare il livello della sicurezza online e la resilienza nel mondo?

Riccardo Bellini: L'accordo stretto tra Microsoft, Facebook e altre 32 aziende tecnologiche mondiali ha l'ambizione di proteggere gli utenti dagli attacchi informatici, indipendentemente dalla nazionalità, dalla geografia o dalla motivazione dell'attacco. Una scelta che è anche una risposta ad un anno che non ha precedenti in fatto di attacchi informatici. Come ha detto Brad Smith, presidente di Microsoft, viviamo in un nuovo mondo, in cui sono presenti nuove tipologie di armi e dove il Cyberspazio è diventato il campo di battaglia. I devastanti attacchi informatici del 2017 hanno dimostrato la necessità per il settore tecnologico di intraprendere un percorso di iniziative più efficaci per collaborare e difendere gli utenti in tutto il mondo.

Il World Economic Forum ha messo la pirateria informatica tra i primi cinque grandi rischi globali dell'economia. I danni finanziari del Cybercrime nel mondo si sono quintuplicati in breve tempo: nel 2011 si contavano circa 100 miliardi contro i 500 del 2017. Per quanto riguarda l'Italia, siamo intorno ai 10 miliardi annui che coinvolgono circa un milione di persone. Dati impressionati se rapportati al quantitativo di denaro che le aziende spendono in sviluppo e prevenzione: da recenti stime infatti solo l'1,5% del budget informatico è destinato alla prevenzione dei rischi.

Questo accordo rappresenta sicuramente un primo passo per contrastare il problema. Nei prossimi anni sarà necessario, non solo aumentare considerevolmente gli investimenti per la sicurezza informatica, ma anche far crescere la cultura su questi argomenti e promuovere la condivisione dei rischi. Spesso, per paura del danno di immagine, le imprese non rivelano le truffe subite, credendo così di ridurre i costi degli attacchi informatici. Attualmente le persone vivono con eccessiva leggerezza il mondo online e questo ha fortissime ripercussioni non solo sulla sfera personale ma anche su quella aziendale. Mi aspetto quindi programmi di sensibilizzazione forti e una crescente tutela degli utenti, ancora ignari dei pericoli in cui incorrono, da parte delle principali aziende tecnologiche mondiali.

05

La pervasività e l'asimmetricità della minaccia informatica non ammette oggi la possibilità di proteggersi completamente contro i Rischi Cyber. L'assicurazione Cyber Risk è già o sarà una soluzione?

Riccardo Bellini: Come detto precedentemente, nell'ultimo periodo sta crescendo la consapevolezza del Cyber Risk e con essa la ricerca di strumenti e servizi volti alla protezione da questi rischi.

Ma di che rischi stiamo parlando? Quando parliamo di Cyber Risk ho in mente, per semplificare, tre tipologie di danni: Danni materiali diretti e indiretti, Danni immateriali diretti e indiretti e Richieste di risarcimento per responsabilità.

Nella prima categoria ci riferiamo, per esempio, a quei danni dovuti al furto o alla distruzione totale o parziale di strumenti informatici quali server, pc, cellulari o altri device che contengono una grossa mole di dati. Con la seconda categoria ci riferiamo invece a danni che toccano beni non tangibili, per esempio un virus che cancella i dati o rende inutilizzabile un server o un dipendente che erroneamente cancella o inoltra dati sensibili ad altre controparti. La terza categoria si riferisce invece alle società fornitrici di servizi informatici che, se colpite da un danno Cyber, ricevono richieste di risarcimento dai loro clienti.

Parte di questi rischi sono già assicurati dalle imprese di assicurazione che, individuato da tempo un nuovo settore di business, hanno iniziato a comprenderli nelle polizze tradizionali ma, dopo l'emanazione del regolamento europeo sulla protezione dei dati (GDPR), sono certo che crescerà vertiginosamente la richiesta di ulteriori tipologie di coperture assicurative e di polizze ad hoc.

A mio parere, le polizze, da sole, non saranno mai una soluzione ai Cyber Risk, per il fatto che non tutto è assicurabile per legge, a maggior ragione in presenza di dolo, ma saranno una indispensabile fonte di tutela per gli investitori, per le aziende e per i loro dipendenti. Certo è che nei prossimi anni, a seconda del settore in cui si opererà e della mole di dati che si tratterà, non ci si potrà esimere dal sottoscrivere una copertura assicurativa, così come oggi non è possibile circolare per strada senza una polizza auto.

NEXTVALUE

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

Il nostro valore è il nostro network, oltre 5.000 Decisori di acquisto – IT e non IT – di aziende end-user in Italia. La community di CIONET Italia è il canale privilegiato attraverso cui conduciamo l'attività di ricerca primaria sui CIO e Direttori IT delle imprese Top e Medio Grandi in Italia.

I nostri Clienti sono 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, nel 2017 abbiamo curato 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