protiviti® Insights

Face the Future with Confidence

Novembre CYBER RISK 2019

a cura di / **Antonio Pantaleo**
Senior Manager

LA SFIDA DELLA QUANTIFICAZIONE DEL RISCHIO CYBER

Cambiano scenari e modelli, “incursori” e attori della protezione e non sempre l’approccio a silos basato sui controlli (regolamentari e non) e sulla sicurezza operativa riesce a precedere nuovi fenomeni.

Se il cyber risk è fra le prime preoccupazioni per le aziende europee (italiane comprese) come indica il report “Regional Risk for Doing Business 2019” diffuso dal World Economic Forum, è opportuno cominciare a porsi qualche domanda: come misurarlo in maniera chiara per tutti gli stakeholder aziendali? Come decidere dove allocare le risorse affinché il ritorno sull’investimento sia massimizzato? Come capisco se ho investito troppo o troppo poco? E soprattutto, quali elementi informativi ed asset sono veramente utili ai fini dell’analisi?

Una prima serie di osservazioni spinge necessariamente a ridefinire il rapporto con le misure di protezione IT, che pur restando la grande area dove si è lavorato e investito finora, non riesce sempre ad evolvere di pari passo con le minacce o ad intercettare tempestivamente i rischi emergenti.

Cambiano scenari e modelli, “attaccanti” e attori della protezione e non sempre l’approccio a silos basato sui controlli (regolamentari e non) e sulla sicurezza operativa riesce a precedere questi fenomeni.

L'EVOLUZIONE DELL'ORGANIZZAZIONE PER LA GESTIONE DEL RISCHIO CYBER

Una delle complessità è che non esistono dei modelli organizzativi effettivamente integrati in cui tutti gli attori della prevenzione e protezione (es. gestori dei Rischi, della Sicurezza, della Compliance a titolo illustrativo e non esaustivo) adottano una base informativa condivisa e comunicano i risultati delle loro analisi in maniera coerente e coordinata.

A ciò va aggiunto che i modelli di business stanno cambiando grazie a un apporto sempre crescente delle tecnologie, per cui ai rischi associati all'innovazione digitale se ne accompagnano altrettanti nuovi di natura IT e Cyber.

Ne deriva la necessità di ridefinire – e non sarà facile – un nuovo modello di gestione del rischio in grado di coniugare obiettivi di sicurezza (ovvero di prevenzione e reazione), misurazione dell' esposizione (ovvero pianificazione e controllo) e comunicazione dei rischi cyber. L'obbiettivo ultimo è quello di (far) comprendere che un rischio cyber è di fatto un rischio di business.

Una tale evoluzione rende necessaria l'introduzione di nuove figure e di nuovi ruoli e non solo un mutamento di funzione dell'esistente, nonché ovviamente di nuovi e più evolute piattaforme tecnologiche a supporto. Tale osservazione vale per tutti, organizzazioni finanziare (e non) e relativi fornitori.

QUANTIFICAZIONE, AFFIDABILITÀ DEI DATI E TEMPESTIVITÀ DELLA COMUNICAZIONE

La quantificazione del rischio, la sua misurazione su scale condivise e la tempestività con cui questa viene analizzata e rappresentata è un tema innovativo in cui una moderna organizzazione finanziaria dovrebbe cimentarsi.

Un argomento importante sul quale focalizzarsi è che spesso tali organizzazioni hanno più dati/informazioni di quanto in realtà sappiano gestire o addirittura necessitino. Dall'esperienza empirica cumulata da Protiviti in materia, appare chiaro che nell'approccio quantitativo la qualità e l'affidabilità dei dati utilizzati assume maggior valore rispetto ai semplici volumi. Questa osservazione dovrebbe prima di tutto indurre le organizzazioni ad abbandonare gradualmente checklist e gap assessment che appaiono inseguire sempre più un concetto di conformità piuttosto che di sicurezza, per focalizzarsi invece sulla definizione di un modello dati integrato, in cui il valore aggiunto delle funzioni dedicate alla prevenzione e protezione non sia la ricerca dell'informazione fine a sé stessa, quanto piuttosto l'insieme delle decisioni sull'uso che si decide di farne ai fini dell'analisi dei rischi.

La visione Protiviti

È soprattutto la capacità di quantificare il rischio cyber la principale chiave di volta che permetterà ai soggetti finanziari di dimostrare agli organi di governo e regulator il più alto livello di consapevolezza e responsabilità, di impostare una più efficiente prevenzione e monitoraggio nonché garantire una più oculata gestione delle eventuali coperture dei rischi da minacce informatiche.

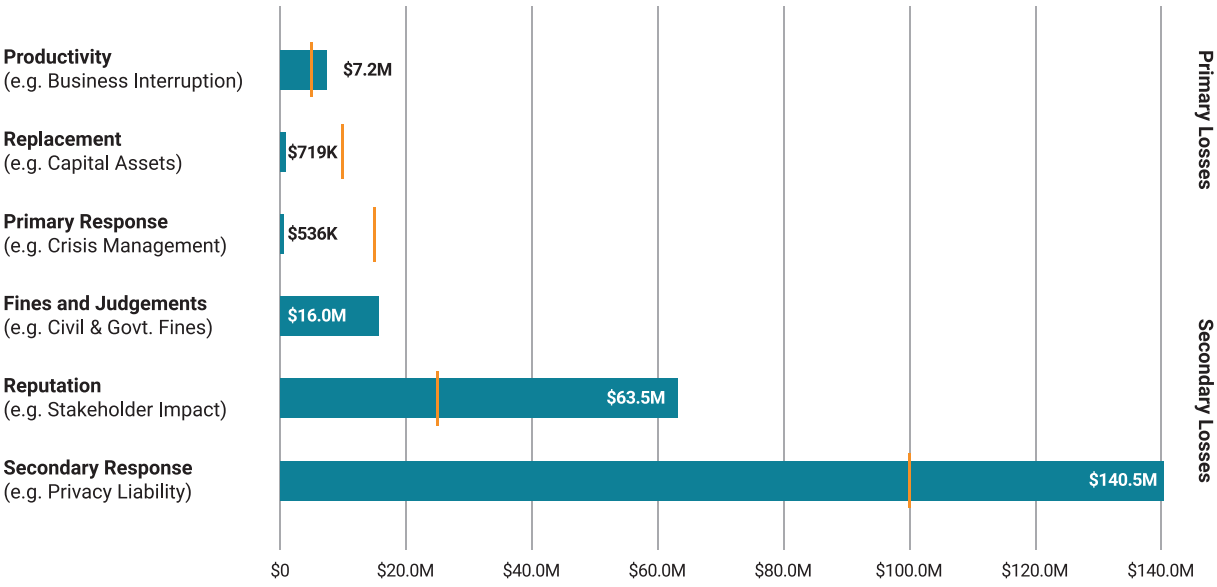
La proposta Protiviti

La scelta di Protiviti di proporre alle aziende la miglior misurazione possibile poggia su una implementazione ad hoc della metodologia FAIR (Factor Analysis of Information Risk), che a sua volta nasce dall'esperienza diretta dei maggiori professionisti della gestione dei rischi IT e Cyber. Oltre a includere le informazioni provenienti dal "mondo dei controlli" e della sicurezza, la metodologia sviluppata prevede di coinvolgere anche gli utenti di business. A questo Protiviti affianca una propria proposta di piattaforma per raccogliere dati in forma strutturata, elaborarli, e sfruttare delle metriche rilevanti ai fini dell'analisi e della reportistica.

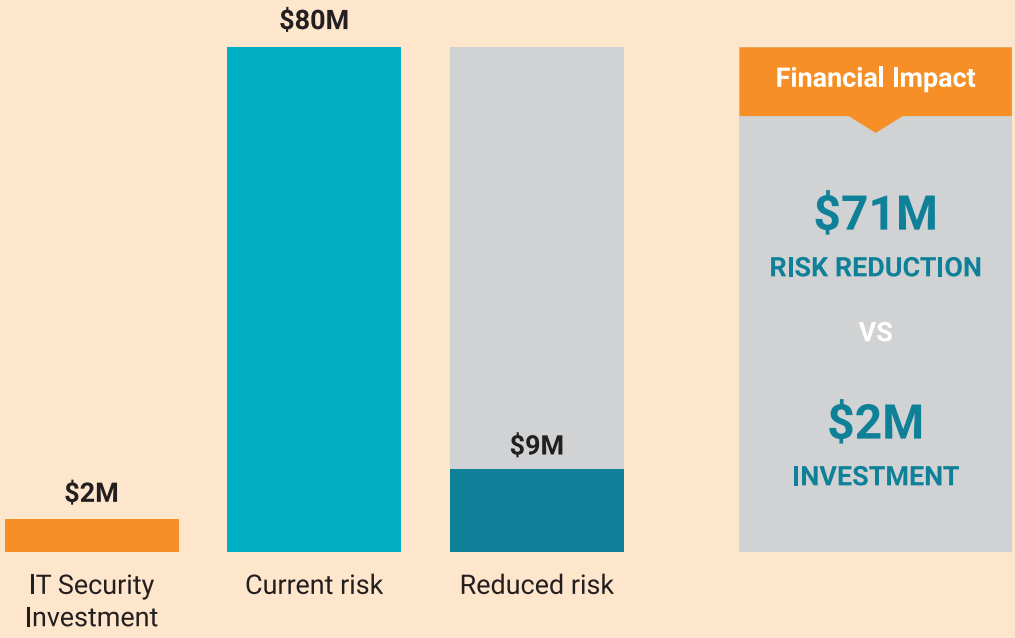
Avremo modo di riprendere questi temi nei prossimi Insights.

IL CONSIGLIO	1. Quantificare	2. Semplificare	3. Informare
	Il rischio cyber può e dovrebbe essere misurato mediante un approccio quantitativo e probabilistico. Metodi matematici e statistici consolidati sono efficaci anche con una quantità limitata di dati.	Il rischio cyber è un rischio di business e, come tale, deve essere analizzato. Il modello proposto consente alle funzioni coinvolte a vario titolo nella gestione dei rischi cyber di collaborare sulla determinazione delle variabili di probabilità ed impatto sulla base di una tassonomia standard.	Focalizzarsi sulle minacce cyber come se gravassero direttamente sugli obiettivi complessivi dell'organizzazione, e sui c.d. *crown jewel*, permette di ottenere un maggiore coinvolgimento degli stakeholder circa le priorità in materia di sicurezza.

"WHAT TYPE OF LOSS CAN WE EXPECT?"



"WHAT IS THE COST/BENEFIT OF THIS PROJECT?"



CONTATTI

— **Antonio Pantaleo** / Senior Manager / antonio.pantaleo@protiviti.it