Interviste

Corporate Security Management: un approccio multidisciplinare e proattivo

Intervista a

Giampaolo Gioia

Corporate Security Management presso un primario Gruppo Aziendale

Buon senso e fiuto per cogliere anche i più deboli segnali di criticità, conoscenza di tecnologie, servizi e norme ma soprattutto capacità di illustrare come stanno le cose e come invece dovrebbero essere. In sostanza: essere manager. Questa l'essenza del lavoro del security manager secondo un veterano come Giampaolo Gioia, Corporate Security Management di un primario Gruppo Aziendale articolato a livello internazionale (indovinate quale).

Communication, Game, Finance, e ancora Logistica, Porti, Aviation, Vigilanza Privata, Close Protection: il suo expertise spazia nei settori più diversi. Qual è il denominatore comune della sua attività? Cosa significa per lei fare Sicurezza Aziendale?
Significa tutelare gli asset e gli interessi dell'impresa, ovvero l'insieme dei fattori competitivi, strutturando un sistema di gestione articolato in specifiche attività manageriali, tecniche e operative. Il denominatore comune delle mie esperienze è l'applicazione di un modello manageriale multidisciplinare capace di cogliere gli aspetti complementari tra le esigenze di Security e quelle di Safety. Ciò impone di organizzare una governance sistemica del rischio orientata alla massima proattività in considerazione dei sempre più numerosi fattori di convergenza tra le problematiche di Security e di Safety.

Anche nel mondo delle tecnologie per la sicurezza si propugna da tempo un modello sempre più integrato tra security e safety. Si può parlare in parallelo di 'governance integrata'?
Organizzare la Sicurezza Aziendale in maniera integrata e interdipendente è essenziale per sviluppare una vera resilienza organizzativa nella gestione delle crisi e delle emergenze. La business continuity è elemento strategico, oltre che imprescindibile, per la sostenibilità dell'impresa. Primaria, a tal fine, è l'analisi di risk assessment: saper valutare correttamente i rischi criminosi, psico-sociali, terroristici, di travel security e saperli porre in relazione con le afferenze della Safety è la base di una governance integrata del rischio. Il primo passo è l'ascolto: riconoscere l'aspettativa di sicurezza dell'utenza cui mi riferisco permette di comprendere sia le più eterogenee istanze in materia di sicurezza (fattuali, aziendali, sociali), sia le peculiarità dei contesti entro i quali le attività dovranno svolgersi.

Il Security Manager è il ponte tra figure professionali eterogenee, tra funzioni aziendali diverse e dunque tra linguaggi diversi

Vanta anche una lunga esperienza nell'Arma: si possono travasare le competenze istituzionali nel mondo della sicurezza privata?
Per lavorare nel privato un'impostazione istituzionale, per quanto solida e specializzata, non basta: occorre una componente manageriale che consenta di percepire nel profondo come vive e funziona un'azienda. Solo penetrando nei gangli aziendali e nei processi rilevanti è possibile far percepire la sicurezza come opportunità di investimento, da tradursi in policies e organizzazione, e non come mero centro di costo. Per far evolvere la sicurezza *da problema a valore aggiunto* aziendale, occorre trovare un modello di proattività al rischio. Come? Elaborando un Documento Programmatico della Sicurezza Aziendale volto non solo alla risposta a situazioni potenzialmente dannose, ma anche alla salvaguardia degli asset e del sostentamento della produttività d'impresa. In tal senso la sicurezza aziendale è un processo iterativo ed evolutivo di valutazione, gestione, mitigazione e riesame dei rischi che si traduce in una serie di fasi e attività progettuali/organizzative/gestionali/operative.

Sotto il profilo umano, che caratteristiche deve possedere il Corporate Security Manager?
Buon senso e fiuto per cogliere anche i più deboli segnali di criticità. E ovviamente saper conoscere – ed usare in maniera compliant - le soluzioni disponibili in termini di tecnologie, servizi e norme. Anche l'aspetto comunicativo è rilevante: occorre saper coinvolgere le persone nei progetti di Security con programmi di security&situation awareness, quindi: prima ancora di saper risolvere problemi occorre saper *spiegare* come stanno le cose e come invece dovrebbero essere. In sostanza: occorre essere manager per svolgere non solo funzioni di controllo e presidio dei rischi ma anche per ricoprire un ruolo di indirizzo strategico e supporto decisionale business risk oriented, in favore dei decision maker e dell'executive board.

Se la capacità di comunicazione è un aspetto essenziale della sua professione, il linguaggio non è però sempre comune a tutti gli interlocutori di riferimento. Mi riferisco ai tecnici, che parlano "tecnichese", al team compliance che parla "legalese", o al team cyber che parla "informatichese". Se non si parla la stessa lingua è difficile costruire progetti comuni...

Il Security Manager è il ponte tra figure professionali eterogenee, tra funzioni aziendali diverse e dunque tra linguaggi diversi: il suo compito è quindi veicolare il concetto che la gestione della sicurezza è un punto di partenza e non di arrivo. Il security manager deve quindi saper condividere razionalità e metodo nell'affrontare le complessità e le incertezze della corporate security. La collaborazione, e non solo dello staff security, è l'elemento chiave di qualunque forma di condivisione. E per capirsi pur usando linguaggi diversi occorre partire da un assunto: il rischio va "spiegato" al pari di una policy o di una procedura.

Facciamo le corna e passiamo al "cigno nero". Cosa succede in caso di attacco, accesso non autorizzato o violazione/failure dei sistemi di sicurezza con conseguente furto, danneggiamento e diffusione di segreti aziendali? Come si attiva la catena delle responsabilità?

Posto che non tutti gli accadimenti dannosi possono essere catalogati come *cigni neri,* qualsiasi organizzazione dovrebbe dotarsi di un modello di crisis management volta a prevenire la maggior parte dei rischi. Il vero banco di prova è la resilienza organizzativa, perché ingloba la quantità di risorse dedicate e la rilevanza delle attività: elementi che sono in funzione delle dimensioni, complessità e vulnerabilità dell'organizzazione. L'approccio preventivo impone anche di individuare la catena delle responsabilità (generalmente attribuite come *funzione* e non come qualifica). Ogni azienda fa scelte diverse, ma di norma ci si orienta su figure apicali con responsabilità strategiche: AD o DiGe, Security Manager, Safety Manager, IT Security Manager, HSE Manager, HR Manager, Responsabile Comunicazione, Relazioni Esterne, Ufficio Legale, Procurement...

Il vero banco di prova è la resilienza organizzativa, perché ingloba la quantità di risorse dedicate e la rilevanza delle attività

Ha ormai praticamente esplorato l'intero mondo della security privata. Dove si vede tra 10 anni?

Da privilegiato, più che da esperto della materia, mi penso tra dieci anni parte di un team di senior advisor specializzati in consulenze per la corporate & business security, impegnato nello sviluppo di progetti di security risk assessment, nella conduzione di audit per la security, nell'organizzazione della travel security e delle attività di corporate intelligence e nella strutturazione di programmi di training e coaching. Chissà.