L'evoluzione del security manager nella distribuzione – 2

contributo di Giuseppe Mastromattei, Head of Security Department H & M

La security aziendale evolve di pari passo con il sempre più veloce cambiamento ed innovamento tecnologico, e con esso cambiano le minacce e i rischi connessi.
Si rende pertanto necessario rivederne i contenuti lasciando definitivamente alle spalle il tipico approccio reattivo: ho un problema, lo risolvo adottando questa determinata soluzione o implementando una nuova attività che sia di supporto a una risposta efficace alla nuova minaccia.
La sicurezza, oggi deve essere un chiaro processo, condiviso e partecipato, affinché possa diventare uno strumento di *governance* efficace allo sviluppo, prima, e alla protezione, dopo, del business.
Si deve pertanto iniziare a parlare di "Sicurezza Partecipata"; ma prima è forse necessario analizzare in dettaglio quello che spesso, all'interno delle organizzazioni, viene troppe volte dato per scontato o peggio ancora, ignorato, ovvero, il "Sistema Sicurezza"
Il Sistema sicurezza è semplicemente un delicato compromesso tra elemento umano, interazioni sociali e supporto puramente tecnologico.
Come queste tre componenti interagiscano tra di loro è praticamente impossibile definirlo in maniera univoca, ma per poter rendere efficace tale definizione potrebbe risultare più semplice un'analisi fatta partendo dal "fallimento del sistema sicurezza".
Immaginiamo di avere un cruscotto su cui sono posizionate tre leve che rappresentano rispettivamente la componente umana, sociale e tecnologica ed utilizzare questo strumento per definire un piano operativo di sicurezza.

Partiamo dall'ultima delle tre: la **componente puramente tecnologica.** In questo caso il Security Manager analizza le offerte presenti sul mercato e, grazie alla tecnologia sempre più "user friendly" (è sufficiente accennare a quante possibilità oggi esistano utilizzando uno smartphone o meglio an-

cora un semplice tablet di ultima generazione) inizia a fare voli pindarici su soluzioni assolutamente idonee alla risoluzione dei problemi. La soluzione tecnologica scelta, spesso ha due fattori di insuccesso determinanti: Il prodotto non si dimostra all'altezza per svariati motivi, troppo complesso o troppo semplice e quindi inefficace ed inapplicabile, o peggio ancora, il fallimento si compie a causa di un coinvolgimento troppo ampio e fuori dalla portata gestionale dell'organizzazione. È il caso in cui la scelta ricade su di un applicativo che necessita di continue implementazioni e risorse dedicate: Il passo fatto è più lungo della gamba.
La perdita di credibilità che ne deriva, ma soprattutto la perdita economica derivante da tale investimento, connessa al non raggiungimento dell'obiettivo, rappresenta il più comune dei casi di fallimento del sistema sicurezza derivante dalla componente tecnologica.

Componente sociale. Qui è ancora più semplice, basti pensare all'onda emotiva successiva al disastro dell'11 settembre.
Ogni momento storico rappresenta un'opportunità di mandato per il responsabile della sicurezza (security manager), se questi è costantemente attento a quello che succede intorno al proprio modello di business. Il fallimento è però sempre dietro l'angolo e l'insuccesso del sistema sicurezza progettato in prevalenza sulla base della componente sociale male interpretata ha di solito un ottimo effetto iniziale ma risulta essere destinato a finire, o meglio a collassare, in tempi brevi a causa della mancanza di argomentazioni valide per gestire tale sistema una volta finita l'emozione iniziale, o meglio conosciuta sotto il nome di crisi.
Prima di affrontare l'ultima e forse la più importante delle tre componenti è opportuno inserire una breve considerazione riguardo il delicato tema delle consulenze esterne. In entrambi i casi in precedenza descritti, spesso si materializzano davanti all'ufficio del security manager fronde di sedicenti

esperti, auto referenziati, possessori di conoscenze sino al quel momento mai rivelate, con le quali porre fine alle problematiche di sicurezza presenti all'interno dell'azienda, sia attraverso l'utilizzo di tecnologie apparentemente innovative e funzionanti sia attraverso dettagliate analisi degli scenari esistenti, ma spesso non coerenti con le reali esigenze.

Il rischio in questi casi di ritrovarsi di fronte ad una pianificazione almeno annuale di incontri, riunioni, gruppi di lavoro, questionari, liste di controllo (check list), ma soprattutto imbarazzanti richieste da fare all'amministratore delegato, risulta essere troppo grande ed assolutamente non accettabile.

Detto questo non me ne vogliano i colleghi, consulenti e lettori, ma tale precisazione si rende necessaria al fine di tutelare quelle professionalità, che con competenza vivono la consulenza come vera e propria partnership supportando l'organizzazione con sistemi efficaci di analisi i cui risultati risultano da subito fruibili per tutte le funzioni aziendali coinvolte nel processo analizzato.

Infine, il fattore umano.

Senza scendere in argomentazioni letterarie e scientifiche, nel caso in esame si possono ricondurre la cause del fallimento del sistema sicurezza a tre cause ben specifiche: l'incompetenza, la corruzione e l'inconsapevolezza.

L'incompetenza è frutto di un'assenza legislativa con la quale vengono chiaramente definite le caratteristiche professionali proprie del security manager. Nonostante vi siano degli standard qualitativi riconosciuti, la formazione certificata del security manager non è richiesta, non essendo un obbligo di legge, dalle aziende che decidono di inserire all'interno della propria organizzazione tale funzione. È noto che spesso si ricorra ad esperti di "sicurezza istituzionale" provenienti dalle Forze di Polizia, con una grandissima esperienza nel campo della criminalità organizzata, ma spesso privi di conoscenze economiche, finanziare ed organizzative proprie di una azienda quotata in borsa.

Questi non rari casi sono facilmente riconoscibili in molte aziende, anche di rilievo internazionale, dove la maggior parte dei dipendenti non conosce personalmente il capo della sicurezza, ma sa benissimo dove sia ubicato l'ufficio o il dipartimento sicurezza, solitamente riconoscibile dalle porte blindate e da sistemi di controllo accessi all'avanguardia.
Senza dilungarsi troppo circa la corruzione è sufficiente individuare il security manager non solo per le competenze specifiche del ruolo ma, soprattutto, per l'integrità morale che necessariamente lo deve contraddistinguere. Questo ruolo, se soprattutto collocato in una posizione apicale all'interno dell'organizzazione aziendale, permette l'accesso ad ogni informazione di importanza strategica ed è pertanto fondamentale che ogni elemento umano del sistema sicurezza (staff, fornitori, consulenti) sia assolutamente di provata lealtà aziendale.
Infine l'inconsapevolezza, o meglio l'incapacità di analizzare obiettivamente ogni tipologia di rischio perché troppo radicato in convincimenti assurdi e pretestuosi.
Una volta determinate le caratteristiche del sistema sicurezza in modo tale da essere abbastanza lontani dalle esaminate cause di fallimento e quindi davanti ad un sistema di sicurezza quantomeno affidabile, inizia quella che è la fase più importante per il consolidamento e riconoscimento all'interno dell'azienda.
Oltre a rimuovere, da subito porte blindate e controllo accessi posti nei pressi dell'ufficio sicurezza è necessario coinvolgere ogni funzione aziendale a supportare un semplice quanto innovativo concetto di sicurezza aziendale: La sicurezza partecipata.
Partiamo dalla definizione.
Sicurezza partecipata vuol dire garantire una maggiore integrazione ed una migliore gestione del rischio, offrendo il massimo contributo a redditività e successo dell'organizzazione stessa. Ovvero, una responsabilità della tutela aziendale non più dispersa o confusa, ma definita in un processo chiaro, condiviso e fruibile per tutti.
Prima però di iniziare è necessario raggruppare tutte le "sicurezze" che spesso operano all'interno delle organizzazioni aziendali senza mai comunicare perché considerate delle attività diverse ed incompatibili tra di loro: un esempio su tutti è la scarsa collaborazione che esiste, nei molti casi in cui sono considerate funzioni ben separate, tra "security" e "safety".
Non è raro imbattersi in accese riunioni durante le quali si scatenano a vere e proprie battaglie tra il Security Manager e il Responsabile del Servizio Prevenzione e Protezione (RSPP): il primo perché pretende che le porte siano ben chiuse il secondo, ovviamente aperte per garantire il deflusso in caso di emergenza!
Raccolte le sicurezze disperse, comprese le componenti tecnologiche (IT), impiantistiche (Building) ed umane (Human Resources) inizia il delicato processo della comunicazione ovvero, definire, all'interno della funzione sicurezza una chiara strategia comunicativa da utilizzare con le altre funzioni aziendali.
Tale strategia dovrà essere incentrata su chiarezza e semplicità degli argomenti trattati e sempre orientata alle esigenze degli interlocutori.
Uno dei più comuni errori da evitare è quello di creare barriere comunicative e, soprattutto, assumere sempre un atteggiamento proattivo durante l'analisi di tutti i processi aziendali. Semplicemente: partecipazione ai processi aziendali rendendo la sicurezza pura funzione di sostegno, offrendo in ogni circostanza il massimo contributo.
Spesso capita di osservare durante incontri di condivisione di progetti o di valutazione di strategie commerciali, il security manager, se invitato, partecipare in silenzio, seduto in un angolo, intento a pensare a tutte le possibili sciagure che potrebbero capitare. Fermo in attesa di prendere la parola con il solo scopo di spaventare, i presenti, i quali dopo un attimo infinitesimale di stupore, ed acquisito in maniera ovviamente inconsapevole il rischio, continuano a discutere del progetto preoccupandosi di tanto in tanto di tranquillizzare il security manager con frasi del tipo: "anche in questo caso siamo consapevoli dei rischi, ma non ti preoccupare ti manderemo ogni dettaglio per le tue valutazioni in merito".
Dettagli che puntualmente non arrivano, salvo casi in cui, malauguratamente, una delle "profezie" si avvera. La strategia comunicativa è pertanto di fondamentale importanza per iniziare il processo di sicurezza partecipata all'interno dell'organizzazione. È ovvio che tutto deve ricevere il giusto consenso ed approvazione da parte dell'amministratore delegato e/o direttore generale, altrimenti ogni tentativo risulterà vano. Ma non subito.

Questo consenso dovrà essere ottenuto solo nella fase finale della strategia comunicativa: focalizzarsi immediatamente sul vertice aziendale è l'errore che più frequentemente viene commesso da inesperti security manager.

Si ritiene infatti che per ricevere un adeguato impegno (commitment), cioè identificazione e riconoscimento del ruolo, sia necessario e sufficiente "spaventare" adeguatamente il vertice aziendale, ipotizzando scenari apocalittici. (grande errore).

L'unico risultato ottenibile con questo approccio è una progressiva identificazione del security manager nel sottotenente Giovanni Drogo che viene assegnato alla Fortezza Bastiani, ultimo avamposto ai confini del Regno, posta a dominio di una desolata pianura chiamata "deserto dei Tartari", un tempo teatro di rovinose incursioni da parte di agguerriti nemici. Tuttavia, da tempo ormai non più minacciata la Fortezza, svuotata ormai della sua importanza strategica, rimane solo una costruzione arroccata su una solitaria montagna, di cui molti ignorano anche l'esistenza. (Il deserto dei Tartari, romanzo di Dino Buzzati. Pubblicato nel 1940).

Si parla pertanto di una vera e propria "comunicazione del rischio", cioè di comportamenti, parole ed altre interazioni che recepiscono e rispettano le percezioni dei destinatari dell'informazione, con lo scopo di fornire appropriati strumenti decisionali per una efficace gestione dei risultati emersi dall'analisi del rischio.

La comunicazione del rischio deve riguardare cosa la sicurezza fa, non solo quello che dice, ma e deve inoltre rappresentare nella forma comunicativa la componente emotiva nella percezione del rischio delle persone, consapevole che questa è diversa per ogni funzione aziendale.

Tale comunicazione sarà più efficace se pensata come dialogo e non come istruzione. Si avrà più successo se l'obiettivo è incoraggiare certi comportamenti, non semplicemente aspettarsi che i destinatari delle informazioni facciano ciò che i comunicatori desiderino.

Tutto ciò sarà possibile se gli obiettivi verranno chiaramente e in precedenza definiti:

· Sviluppare la conoscenza e la comprensione;
· Aumentare la fiducia e la credibilità;
· Prevenire e risolvere conflitti.

Tutto ciò adottando una terminologia semplice e un linguaggio chiaro, mantenendo costante la trasparenza degli obiettivi e delle strategie seguite durante ogni fase dell'analisi del rischio, condividendo la strategia e gli aspetti operativi di interazione con tutte le parti interessate e rendendo pubblici i risultati derivanti dall'analisi del rischio e delle politiche.

Il processo di comunicazione è probabilmente il più complesso da gestire in tutto il ciclo dell'analisi del rischio, difficile da generalizzare per quanto riguarda metodo e approccio ed è fortemente dipendente dalle condizioni sociali, economiche, culturali e politiche.

Sarà pertanto determinante agire sulla comunicazione del Rischio consapevoli dell'importanza della stessa al pari dell'analisi e della gestione del rischio stesso, all'interno di un unico e condiviso universo del rischio.

In un mondo in cui la velocità dei cambiamenti non è più controllabile, la Sicurezza diventa pertanto una questione di partecipazione e controllo dei processi aziendali in modo tale da poter consentire all'azienda di continuare a sviluppare e mantenere il proprio business in maniera sempre più consapevole ed efficace.

La sicurezza partecipata come strumento efficace di governance deve essere pertanto considerata un sistema fruibile e condiviso da ogni funzione aziendale per mantenere un'adeguata capacità competitiva superando eventuali incidenti con un approccio costantemente sempre consapevole per tutta l'organizzazione.

"La potenza è nulla senza controllo", era un famoso slogan pubblicitario degli anni passati, e un'azienda senza un chiaro sistema di *governance* non potrà rimanere competitiva negli anni. Soprattutto negli anni futuri.