WORKSHOP

LA PARTNERSHIP PUBBLICO – PRIVATO E LA FUNZIONE DI SECURITY MANAGER

Roma, Scuola Superiore di Polizia

13 novembre 2012

INTERVENTO
di Damiano Toselli
(Presidente A.I.P.S.A.)

LE PROSPETTIVE DELLA SECURITY AZIENDALE

A.I.P.S.A

L'AIPSA (**Associazione Italiana Professionisti Security Aziendale)** è un'associazione senza fini di lucro, nata negli anni '80 per volontà di un gruppo di Security manager. Attualmente riunisce 270 iscritti, in rappresentanza delle maggiori aziende italiane.
Ha come **obiettivi istituzionali**: la valorizzazione dell'ordinamento professionale, la formazione e l'aggiornamento costante degli associati, la diffusione della cultura della security e l'approfondimento dello studio delle sue problematiche di ordine tecnico, funzionale, giuridico e legislativo.
Per realizzare i suoi obiettivi, l'AIPSA fa parte di numerosi e diversificati enti del settore sicurezza, attraverso i quali realizza le sinergie necessarie al raggiungimento degli obiettivi strategici, di volta in volta, indicati in programmi triennali; mantiene inoltre stretti legami di collaborazione con altre associazioni del settore sicurezza.
Nel 1995, l'AIPSA ha contribuito in modo determinante alla ratifica della **Norma UNI 10459** sulla "Funzione e profilo del professionista della Security Aziendale".

Evoluzione della security

La globalizzazione dei mercati, l'internazionalizzazione del business, la continua evoluzione tecnologica sono solo alcuni degli aspetti che hanno determinato la nascita di **nuovi rischi** per la società in generale e per le imprese in particolare. Tutto ciò ha portato le aziende ad istituire, all'interno della propria organizzazione, la funzione di Security in maniera sempre più strutturata rispetto al passato.

Gli **asset** e i **"confini"** da tutelare si sono trasformati, rendendosi, il più delle volte, **intangibili**. Tutto questo si traduce in **nuove sfide** per la sicurezza pubblica e per la sicurezza aziendale, accentuando la necessità di partnership sempre più efficaci.
L'impresa è un soggetto economico che incide direttamente sul benessere e sullo sviluppo del territorio in cui opera, contribuendo direttamente alla qualità di vita della comunità di riferimento. **Tutelare l'Azienda**, salvaguardare le sue risorse (umane, economiche, infrastrutturali, …) significa quindi **contribuire a sviluppare**, insieme agli altri soggetti pubblici e privati, **la "rete" di tutela del "Sistema-Paese".**
In Italia, il ruolo del Professionista di Security Aziendale ha subito una continua evoluzione, adeguandosi al contrasto dei nuovi fenomeni criminali e fraudolenti, che si sono manifestati negli ultimi decenni.
Ripercorrendo in breve la storia della Security aziendale in Italia, possiamo osservare che negli **anni '70**, la priorità era proteggere i Vertici aziendali dal terrorismo e dai sequestri di persona; erano necessarie quindi le competenze professionali specialistiche di security; di fatto, è proprio in questo periodo che nasce la Security presso le aziende.
Negli **anni '90**, i primi sviluppi delle nuove tecnologie telematiche hanno evidenziato la necessità di proteggere le informazioni; vi è stato un riordino della security, in linea con gli standard delle multinazionali, che riconosceva l'importanza della **Security Intelligence** anche nei settori del business.
Dal **2000** fino ad oggi, la security aziendale ha dovuto affrontare criticità legate ad organizzazioni criminali trasnazionali, sia di matrice terroristica sia mafiosa, che, colpendo target civili e indifesi, hanno posto alle aziende problemi di protezione del personale in occasione di grandi eventi aziendali e di viaggi di lavoro (in particolare in alcune aree geografiche "a rischio"). Inoltre l'espansione di internet ha richiesto di potenziare la **Cybersecurity**.
Un aspetto fondamentale di questo periodo è lo **sviluppo della "Sicurezza Partecipata"**, testimoniato dall'aumento del numero di **Convenzioni stipulate tra FF.OO. e Aziende**, tra cui:

ANMIL Onlus - Via A. Ravà, 124 - 00142 Roma
Tel. +39 06 54196334/208 - fax +39 06.5402248 - comunicazione@anmil.it - www.anmil.it

- la *"Convenzione tra il Dipartimento della Protezione Civile e i fornitori dei servizi di comunicazione elettronica per la fornitura di informazioni d'emergenza nelle aree geografiche nazionali";*
- la *"Convenzione per la prevenzione dei crimini informatici sui sistemi di gestione per le infrastrutture critiche di telecomunicazioni dipendenti dalla Telecom Italia S.p.A."*;
- la *"Convenzione tra l'Unità di Crisi del Ministero Affari Esteri e gli operatori dei servizi di comunicazione elettronica per la fornitura del servizio di invio di messaggi ai cittadini italiani all'estero per i casi di emergenza",* tra Ministero Affari Esteri, Ministero delle Comunicazioni e le società Telecom Italia, Vodafone, Wind, H3G;
- il *"Protocollo d'intesa per l'istituzione dell'Osservatorio nazionale sui furti di rame"* tra Ministero dell'Interno, Agenzia delle Dogane, Ferrovie della Stato Italiane S.p.A., Enel S.p.A., Telecom Italia S.p.A., Anie.

Nel contempo, si assiste ora ad una costante riduzione del ruolo dello Stato in molti settori e, parallelamente, i privati sono diventati proprietari di molti asset strategici. La nostra società sta diventando sempre più dipendente da sistemi altamente distribuiti su larga scala, che operano in reti senza confini ben definiti. **Infrastrutture** come le reti di telecomunicazione, le reti di energia (elettricità, gas, …), le reti di trasporto, il sistema sanitario, o i circuiti bancari e finanziari, sono ormai divenute indispensabili per il lavoro e lo sviluppo della nostra società. La mancanza dei servizi erogati da tali infrastrutture porterebbe in tempi brevi portare alla paralisi del Paese: proprio per questo, vengono dichiarate **"*critiche*".**
Fino a qualche decennio fa, ognuna di queste infrastrutture poteva considerarsi un sistema autonomo, sostanzialmente indipendente e gestito da operatori verticalmente integrati. Oggi le varie infrastrutture tendono ad essere sempre più strettamente connesse, al punto che esse risultano **interdipendenti**. Ciò comporta che un guasto (di natura accidentale o dolosa) in una di loro può facilmente propagarsi con un **"effetto domino"** alle altre, amplificando i suoi effetti e provocando disfunzioni e malfunzionamenti anche ad utenti remoti, sia dal punto di vista geografico che funzionale, rispetto a dove si era originariamente generato il guasto. Alla luce di queste considerazioni l'attenzione del Security Manager, ma anche degli altri manager aziendali, verso le tematiche di **Business Continuity** e di **Crisis Management** è cresciuta.
Negli ultimi anni, la crescente consapevolezza del ruolo determinante della sicurezza per lo sviluppo del business (**security** sempre più **"business oriented"**) è testimoniata anche dall'ampliamento della struttura e dalla crescita del livello della Security nell'organigramma aziendale: nella maggior parte delle imprese italiane medio-grandi è collocata **a diretto riporto del Vertice** (e non come era all'inizio degli anni '70, inserita in funzioni non strategiche con i soli obiettivi di "sicurezza fisica").
L'elevata collocazione organizzativa significa anche il riconoscimento che la sicurezza in azienda non può essere un obiettivo della sola Funzione di Security; la Security fa parte infatti di un sistema aziendale integrato, che comprende l'Audit, la Safety, il Legale e che assicura la tutela di tutte le risorse aziendali dai rischi non competitivi. In questo contesto, la partnership tra Pubblico e Privato si è trasformata quindi in un "sistema aperto" di integrazione, collaborazione, interdipendenza, e la **Security** si è presentata come **snodo e interfaccia tra l'Azienda e le Istituzioni**.

Aspetti normativi

La Security aziendale è disciplinata da un chiaro sistema normativo, determinatosi a partire dalla fine degli anni '90, i cui testi principali sono: il Codice Privacy; il D.Lgs. 8 giugno 2001, n. 231 sulla Responsabilità d'Impresa; il D.Lgs. 81/2008 sulla sicurezza nei luoghi di lavoro; il Sarbanes/Oxley Act per tutte le società quotate in U.S.A., la Direttiva Europea sulle Infrastrutture Critiche in vigore dal 12/1/2009. Oltre a questi testi, ci sono alcune normative settoriali, tra cui: il Codice TLC; la Legge 217/1992 per gli Aeroporti; il DM 269/201 per il Regolamento Istituti di Vigilanza.

Rapporti tra Istituzioni e Aziende

Quanto sopra potrà anche consentire di valutare la necessità di una rimodulazione del sistema normativo, che superi le **asimmetrie legislative in campo internazionale** in vari settori (privacy, regolatorio, commerciale,…) al fine di consentire, nel contesto della globalizzazione, una corretta concorrenza. La rimodulazione del sistema normativo dovrà anche tener conto della necessità di un sistema di relazioni tra Pubblico e Privato più ampio, più integrato, che faciliti, nel chiaro rispetto dei ruoli e delle funzioni, maggiori sinergie operative e, quindi, possa diventare **un sistema di collaborazione non solo più efficace, ma anche meno costoso**.
Nelle organizzazioni complesse sopra richiamate, sia istituzionali che aziendali, che fanno parte del Sistema-Paese, appare evidente la difficoltà di semplificare, tuttavia si manifesta la necessità di individuare **"Focal**

ANMIL Onlus - Via A. Ravà, 124 - 00142 Roma
Tel. +39 06 54196334/208 - fax +39 06.5402248 - comunicazione@anmil.it - www.anmil.it

Point" istituzionali per mantenere, tra Azienda e Istituzioni, rapporti a livello formale ed informale, mentre si impone di mantenere comunque una chiara separazione di ruoli, poteri, competenze.
Il continuo sviluppo della collaborazione tra Pubblico e Privato consentirebbe inoltre di ridurre le spinte private all'autotutela, recentemente manifestatesi in varie forme, nonché di mitigare le "gelosie" istituzionali mirate alla salvaguardia delle proprie prerogative.
Si sottolinea infine che la collaborazione tra Aziende e FF.OO. richiede anche una maggiore **standardizzazione del monitoraggio**, la **condivisione di database** e un **approccio comune ai metodi di prevenzione**.

Formazione e fattori di successo

Da quanto sopra richiamato, appare evidente la necessità di garantire ai professionisti della sicurezza aziendale una **formazione continua**, sia per i ruoli specialistici e tecnici, sia per i ruoli manageriali. La formazione e la sensibilizzazione del personale (corsi, testing, esercitazioni), nonché la partecipazione alle iniziative di cooperazione organizzate dagli Organismi istituzionali dello Stato (esercitazioni, mostre, fiere, convegni), sono attività necessarie all'implementazione del sistema di gestione della sicurezza in azienda. Sotto il profilo professionale, per il security manager la **correttezza** si declina in capacità di non creare "falsi allarmismi", per poi fingere di risolverli; la **trasparenza** si traduce nella necessità di "tracciabilità" oggettiva di tutti i processi e di disponibilità ai controlli interni; la **riservatezza** significa saper tutelare solo le informazioni critiche.

Comunicare Sicurezza

La comunicazione è un aspetto fondamentale della gestione della sicurezza, sia all'interno che all'esterno dell'azienda. Questo assunto è particolarmente evidente in caso di gestione di un'emergenza: vi è, da un lato, la necessità di comunicare in tempo reale, rapido, tanto più rapido quanto più grave è l'emergenza manifestatasi; dall'altro l'esigenza di attendibilità della comunicazione, quindi di scambio di dati che siano credibili, su cui poter lavorare, su cui poter fare delle scelte.

Costi della sicurezza

La sicurezza è un investimento, ma è anche un costo. Il paradosso della crisi che stiamo vivendo è la necessità di ridurre i costi della sicurezza mantenendo inalterata l'ampiezza del perimetro da proteggere.
In tempi di crisi, ridurre i costi significa dover utilizzare meglio le risorse disponibili, anche all'interno della collaborazione Pubblico-Privato; significa anche saper attingere a fondi e finanziamenti europei stanziati per la sicurezza (PON, Progetti europei, …).

Prospettive

Si possono tracciare le seguenti prospettive di sviluppo:

- superamento della visione, pur positiva, di una "Sicurezza Partecipata";
- acquisizione di una maggiore conoscenza dei rischi e degli strumenti di contrasto nell'ambito della **Cybersecurity** e miglioramento dell'efficienza dei C.E.R.T. (Computer Emergency Response Team);
- incremento delle attività di **Business Intelligence**, per supportare le aziende che operano all'estero e garantire la tutela delle loro risorse umane e delle loro strutture ed impianti.

Conclusioni

E' evidente una maggiore richiesta di sicurezza da parte della società e delle aziende.
Il ruolo dello Stato nel garantire sicurezza è insostituibile. Nelle imprese, la Security assume un ruolo chiave, sia all'interno dell'organizzazione aziendale, sia all'esterno come Focal Point per le Istituzioni.
In questo contesto, la partnership tra Sicurezza Pubblica e Sicurezza Industriale diventa un fattore determinante per lo sviluppo del Sistema-Paese.

ANMIL Onlus - Via A. Ravà, 124 - 00142 Roma
Tel. +39 06 54196334/208 - fax +39 06.5402248 - comunicazione@anmil.it - www.anmil.it