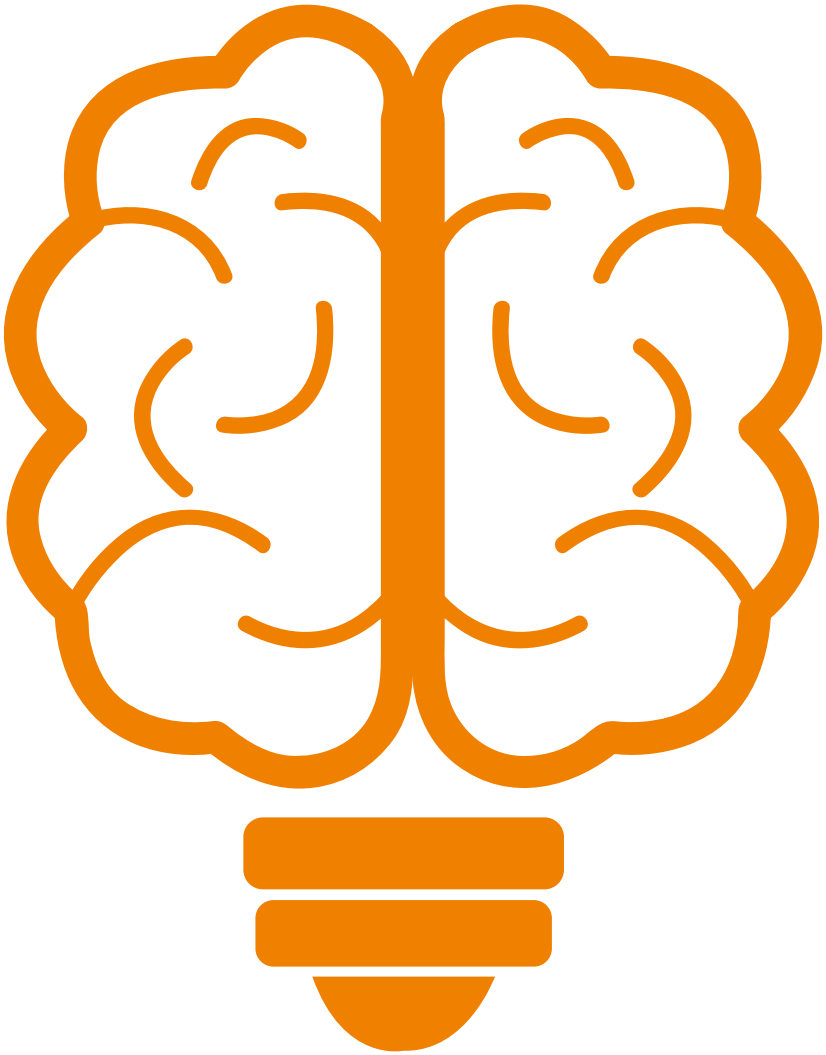
a&s ITALY
Tecnologie e soluzioni per la sicurezza professionale
www.asitaly.com
dicembre 2015
anno VI 36



a&S ITALY
www.asitaly.com
MAGAZINE

IP Security MAGAZINE
www.ipsecuritymagazine.com
MAGAZINE

secsolution
security online magazine
www.secsolution.com
WEB

IP Security FORUM
www.ipsecurityforum.it
EVENTI

festival ICT
www.festivalict.com
FIERE

ETHOSACADEMY
www.academy.ethosmedia.it
TRAINING

INNOVAZIONE NELLA COMUNICAZIONE

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

Ethos Media Group s.r.l.
Via Venini, 37
20127 Milano (Italy)
ethos@ethosmedia.it

www.ethosmedia.it

Alessandro Lega(*)

La Resilienza delle organizzazioni, puntata # 1

Dopo aver trattato i temi della *Security Convergence* un paio di anni fa e la *Protezione delle Infrastrutture Critiche* e il *Security Liasion Officer* l'anno passato, per il 2015 la redazione di *a&s Italy* propone un filone tematico innovativo, che guarda al futuro con un respiro ampio, capace di interessare tutti coloro che guardano al Risk Management come un primo e basilare sostegno al business. Alessandro Lega, al quale ci eravamo rivolti già gli anni passati, ha individuato un argomento che è logica evoluzione di quelli precedentemente trattati e si pone quindi come "terza dimensione" della Gestione del Rischio. Il tema è quello della *Resilienza Organizzativa*.

(*)Senior Security Consultant, CPP ASIS.

L'argomento "Resilienza" potrebbe essere visto sotto diversi punti di vista.

Nella tecnologia dei materiali, la Resilienza è intesa come "la resistenza a rottura per sollecitazione dinamica, determinata con apposita prova d'urto". Al valore di Resilienza viene contrapposto l'indice di fragilità. Qualcosa di simile nella tecnologia dei filati e dei tessuti, dove Resilienza viene associato a "l'attitudine di questi a riprendere, dopo una deformazione, l'aspetto originale". Più genericamente la Resilienza è definita come la "capacità di un materiale di assorbire energia elasticamente quando sottoposto a un carico, o a un urto, prima di giungere a rottura".

Fin qui, un concetto dunque squisitamente fisico, riferibile ai materiali e alle loro caratteristiche di "resistenza". La Resilienza di un'organizzazione è, per similitudine: "la velocità con cui un'organizzazione (o un sistema) ritorna al suo stato iniziale, dopo essere stata sottoposta a una perturbazione che l'ha allontanata da quello stato; le alterazioni possono essere causate sia da eventi naturali, sia da attività antropiche". Le citazioni virgolettate provengono tutte dall'enciclopedia Treccani online.

RESILIENZA DELLE ORGANIZZAZIONI

In questo articolo, e nei successivi, vorrei parlare della Resilienza delle Organizzazioni e degli stretti legami con le diverse discipline organizzative, fra cui la *Security*, da cui ha dirette dipendenze, ma che non è la sola disciplina che concorre a sostenerla. Un punto va subito messo in evidenza: a differenza di discipline specialistiche, quali il *Risk Management*, la *Security*, la *Business Continuity*, il *Crisis Management*, il *Disaster Recovery*, la *ICT Security*, il *Loss Prevention* e tutte le discipline che necessitano la presenza di un leader capace di far funzionare il singolo processo, quando parleremo di Resilienza Organizzativa dovremo immaginare che si tratta di una caratteristica strutturale della organizzazione; di un risultato ottenuto tramite l'integrazione di tanti altri fattori. Quindi non è un processo da governare ma il risultato di tanti processi che insieme contribuiscono a raggiungere un livello più o meno alto di Resilienza Organizzativa, o come preferiscono chiamarla gli anglosassoni: *Organizational Resilience* (OR). Di conseguenza l'attività di management della Resilienza Organizzativa si esplica attraverso la gestione di tutti i processi che sostengono il raggiungimento del più alto livello di Resilienza, da non intendersi una situazione statica, bensì soggetta a continui cambiamenti derivanti da contesti interni e da quelli esterni. Qualcuno potrebbe subito porre la domanda: allora per la Resilienza Organizzativa non occorre un leader? Siamo abituati a vedere soluzioni organizzative che sono basate sulla responsabilità affidata ad un leader. Abbiamo il leader della Total Quality, quello della Compliance, quello dell'Audit, quello della Security. Com'è possibile che possa esistere un qualcosa di organizzativo senza un leader dedicato a gestirlo? In effetti un leader esiste anche per la Resilienza Organizzativa, anzi ne esistono anche più di uno! Tutti i soggetti che interagiscono in una struttura organizzativa hanno un ruolo gestionale agli effetti della Resilienza Organizzativa.

ASPETTI ARCHITETTURALI

Ma facciamo un piccolo passo indietro e vediamo di costruire delle solide fondamenta prima di andare troppo in avanti. Il concetto di Resilienza Organizzativa è fortemente dipendente dalla capacità di gestire il rischio. Solo attraverso un solido processo di Risk Management è possibile individuare, classificare, verificare, mitigare le insidie che possono minare la Resilienza di un'organizzazione. Questo aspetto dovrebbe immediatamente richiamare alla mente che il modello organizzativo del Risk Management

si basa su un processo ben consolidato e ben inquadrato da uno standard internazionale ben conosciuto agli addetti ai lavori: la ISO 31000.

Anche dal punto di vista della definizione ci può venire ancora in aiuto uno standard ISO. La ISO CD Guide 73 - Vocabulary , al punto 3.8.1.7 definisce la Resilience come "adaptive capacity of an organization in a complex and changing environment". Locuzione che mette in evidenza tre cose (in grassetto): la **Capacità** di un'organizzazione in grado di **Adattarsi** in un ambiente **Complesso e Evolutivo**. Di conseguenza, questa **Capacità** (competenza) di **Resistere** (ai rischi) in **Ambiente Complesso e Evolutivo**, può riferirsi a qualsiasi tipo di organizzazione (grande, piccola, pubblica, privata, governativa, ecc).

LE SFIDE

Come sopra descritta, la Resilienza Organizzativa si deve confrontare con diverse "sfide". Sfide tipiche di un ambiente complesso e in evoluzione, che partendo dal Risk Management, passa agli aspetti Finanziari, a quelli di Security, di Comunicazione, della Ricerca, del Disaster Recovery, della Business Continuity, della Reputazione, della Gestione Operativa, dell'Opinione Pubblica, del Crisis Management, dei Rapporti Sindacali e forse la più insidiosa, che è rappresentata da una falsa sicurezza del tipo: "a noi non è mai accaduto….", come spesso si sente ripetere nelle organizzazioni. Un contesto così complesso e in costante evoluzione non può quindi essere affrontato con modalità mono-disciplinari e, ancor peggio, mono-culturali. Ecco perché l'espressione anglosassone "silod" (da silos, contenitore verticale) riferito ad una organizzazione è considerata il modello organizzativo meno adatto per gestire la Resilienza Organizzativa. Come già messo in evidenza in passato a proposito di considerazioni sull'Enterprise Risk Management (ERM), piuttosto che sull'Enterprise Security Risk Management (ESRM), e su Security Convergence, un approccio olistico è la risposta più adeguata per garantire un risultato adeguato, piuttosto che un approccio verticale e settoriale.

CHI È IL LEADER?

E chi è in grado, in un' organizzazione, di far sì che siano eliminati i "silos" organizzativi? A far sì che le varie funzioni aziendali siano motivate e interessate a comunicare fra di loro, collaborando tutte insieme a rendere più robusta l'organizzazione? L'unico in grado di farlo è il c.d. "Vertice Aziendale". Colui, o coloro, che hanno diretta responsabilità nel raggiungere tutti gli obiettivi che l'organizzazione si è posta. Concretamente, solo chi si trova nella posizione di dirigere tutta "l'orchestra" è in grado di farla lavorare all'unisono, indicando le giuste priorità e assegnando le appropriate risorse. Quale risulta essere la principale motivazione di colui/coloro interessati a raggiungere tutti gli obiettivi che l'organizzazione si è posta? Per prima, la riduzione dei possibili impatti che possono derivare dai rischi che circondano l'organizzazione. Ma quali sono i rischi di cui il vertice dell'organizzazione deve tener conto? La risposta è semplice: di tutti i rischi che possono ridurre la possibilità, a breve, medio e lungo termine, di raggiungere i risultati che un'organizzazione ha fissato. Credo si cominci a delineare in modo più completo, e con immediato riflesso sul business, quale sia l'importanza della Resilienza Organizzativa per chi debba governare il presente ed il futuro di un'organizzazione. Non si tratta di un qualcosa che si limita ad una *best practice*, che può essere opportuno adottare. Non è un accessorio bello ma poco utile. E' una necessità essenziale che richiede tutta l'attenzione del vertice organizzativo e che, in caso di ambienti complessi, esige un leader di riferimento in grado, tramite i legami ai vari standard che sono stati predisposti, di divulgare le opportune informazioni e provvedere a diffondere la necessaria *awareness* per ottenere i comportamenti richiesti. Interrompiamo qui questa puntata, ribadendo che a sostegno di tutto ciò che riguarda la Resilienza Organizzativa c'è il processo di Risk Management, di cui parleremo nella prossima puntata.

Alessandro Lega(*)

La Resilienza delle organizzazioni, puntata # 2

Nella puntata precedente ci siamo lasciati con la convinzione che la Resilienza Organizzativa sia basata sulla capacità di un'organizzazione di gestire il processo di Risk Management e che il riferimento più solido sia rappresentato dallo standard ISO 31000. In questa puntata facciamo un passo avanti, inserendo un concetto molto importante, ossia che la Resilienza Organizzativa si pone l'obiettivo di rendere un'organizzazione più resiliente e meglio preparata ad affrontare le criticità derivanti dai rischi. Quindi, l'identificazione, la catalogazione e la prioritizzazione di come affrontare i rischi rappresentano il primo tassello per assicurare la gestione di un management system in grado di creare un'organizzazione resiliente. La parola all'esperto Alessandro Lega.

(*) CPP

Da oltre cinque anni in Nord America è stato adottato uno standard che ha come obiettivo proprio questo aspetto. Con il titolo *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirement with Guidance for Use, l'American National Standards Institute (ANSI)* ha rilasciato l'ANSI/ASIS SPC.1-2009, uno standard perfettamente allineato con ISO 9001:2000, ISO 14001:2004, ISO/IEC 27001:2005, ISO 28000:2007 e ISO31000, ovviamente. Dal 2010 il Department of Homeland Security Americano (DHS) l'ha adottata come *Voluntary Standard* in materia di Resilienza Organizzativa. Di recente, a fine novembre 2014, anche il British Standard Institute (BSI) ha rilasciato un nuovo standard, il BS 65000:2014, che rappresenta il primo vero riferimento alla Resilienza Organizzativa rilasciato in Europa. Anch'esso fa riferimento all'ISO 31000 e all'ISO Guide 73:2009, oltre a molti altri British Standard. Questo fa capire come stia crescendo l'attenzione sull'argomento, cosa confermata anche dai lavori messi in cantiere da ISO con il gruppo TC 223.[1] Come si può ben capire, da questa caleidoscopica visione di standard e norme volontarie, la Resilienza Organizzativa gode di un'ampia letteratura per quanto riguarda le soluzioni organizzative che possono essere adottate per raggiungerla. Fin quando uno standard e le relative certificazioni cui fanno capo rimarranno *volontarie,* e così variegate, si potrà correre il rischio di seguire percorsi diversi per raggiungere risultati che dovrebbero essere comunque coincidenti. Un aspetto, in effetti, accumuna tutto quanto sia stato rilasciato finora in materia di standard riferibili alla Resilienza Organizzativa: riguarda la convinzione comune che sia richiesto un approccio multi disciplinare e multi funzionale. In particolare si può dire che, guardata da tutti i punti di vista possibili, la resilienza viene considerata non come il risultato di una singola disciplina, bensì come una mescolanza di approcci nel guardare ai rischi che possono ridurre la possibilità di raggiungere gli obiettivi che l'organizzazione si è prefissa. In attesa di avere, in un futuro non lontano (qualcuno indica entro il 2017 e noi ce lo auguriamo), un unico standard internazionale di riferimento in materia di Resilienza Organizzativa, ci dobbiamo convincere che il principale sforzo che il top management può fare è quello di far dialogare fra di loro le varie funzioni interne, rimuovendo i separatori che dividono le esperienze e le competenze dei vari settori che compongono l'organizzazione. I c.d. "contenitori" verticali (silos) che tanto danneggiano le organizzazioni perché impediscono che si possa allargare la base di conoscenza dei possibili rischi e delle migliori modalità per poterli mitigare. Quindi quelle organizzazioni che hanno a cuore la loro crescita con una costante attenzione alla riduzione dei rischi, fanno bene a responsabilizzare tutti coloro che devono condividere un obiettivo comune: come sostenere la resilienza dell'organizzazione.

ANSI/ASIS.SPC.1-2009

Senza voler privilegiare uno piuttosto che un altro degli standard, considerando che l'ANSI/ASIS.SPC.1-2009 ha cominciato per primo a parlare in modo specifico di Resilienza Organizzativa, propongo di partire da questo per analizzare i legami che esistono con la ISO 31000. Un'analisi condotta in termini di capacità delle organizzazioni di adeguarsi al cambiamento del contesto di riferimento. Nella prossima puntata faremo poi lo stesso con la BS 65000:2014.

La ISO 31000 è considerata la principale innovazione nel mondo del Risk Management. Definendo i principi, il quadro di riferimento e il processo del Risk Management, la ISO 31000 sposta la visione da un singolo episodio avverso la più ampia incertezza di poter raggiungere nel tempo gli obiettivi che l'organizzazione intende porsi. Quindi il rischio non più visto come singolo episodio su cui concentrarsi ma come percorso per garantire il raggiungimento degli obiettivi, attraverso la gestione dei rischi. Questo vuol dire un'organizzazione meno reattiva ma più proattiva, capace di attivare un processo che vede tutti i possessori di rischi, di una stessa organizzazione, diventare dei Risk Manager. Questo concetto di corresponsabilità nell'identificazione dei rischi è stata fatta più volte nel corso di questa e della precedente puntata. Sarà forse il caso di approfondire questo aspetto per non correre il rischio, tanto per rimanere in materia, che possa apparire un modo di dire senza che dietro ci siano solide basi supportate da una lungimiranza manageriale. Prendiamo per esempio l'individuazione dei ri-

[1] In effetti nel corso degli ultimi anni ci sono stati altri tentativi per affrontare l'argomento, anche se in ambito molto specifico. Per esempio la ISO 22301 che si occupa di Gestione della Continuità Operativa, così come l'Australian Standard AS/293-2006. Più di recente, nel gennaio 2014, UNI ha pubblicato, riferita alla resilienza delle infrastrutture critiche, la Prassi di Riferimento UNI/PdR 6:2014 che si riferisce anche alla ANSI/ASIS APC.1-2009.

schi, delle vulnerabilità, delle minacce, delle probabilità, delle criticità, che sono gli elementi che devono essere analizzati per effettuare un'efficace Risk Analysis da cui deriveranno decisioni su come trattare i rischi a cui l'organizzazione può trovarsi soggetta. E' abbastanza intuitivo comprendere che un'attività congiunta da parte di tutti coloro che si trovano nelle migliori condizioni per individuare e valutare un singolo rischio sarà in grado di dare il miglior contributo per ridurne gli effetti, attraverso la valutazione di tutto ciò che a quel rischio è riconducibile, comprese le modalità per mitigarlo. Se questo processo riesce a coinvolgere tutti coloro che sono a contatto con i rischi, in ogni istante, ne deriva che una condivisione del metodo e delle modalità di trattamento della gestione del rischio potrà garantire una maggiore capacità di individuare, in anticipo, le possibili condizioni avverse all'ottenimento degli obiettivi dell'organizzazione. Allargando questo concetto all'intera sfera del Risk Management e ribadendo l'importanza di adottare una modalità proattiva, anziché solo reattiva, si potrà meglio comprendere come questo sia un processo di tipo consultivo e collaborativo, che vede tutti gli attori "*proprietari*" di rischi essere pienamente coinvolti nella gestione del rischio stesso. Ecco perché coloro che adottano modelli organizzativi capaci di garantire una robusta Resilienza Organizzativa preferiscono modelli manageriali in grado di facilitare comunicazioni top-down, bottom-up e peer-to-peer, attivando un processo capace di coinvolgere il maggior numero possibile di soggetti appartenenti all'organizzazione.

Lo standard ANSI/ASIS.SPC.1-2009 adotta in pieno questi principi, introdotti per la prima volta da ISO 31000. Lo fa mettendo in evidenza il fatto che, per essere resiliente, un'organizzazione deve avere la capacità di adattarsi, nel tempo, alle variazioni che intervengono nei contesti interni e esterni. Per essere in grado di cogliere il massimo delle opportunità e minimizzare le probabilità e le conseguenze di possibili vulnerabilità e minacce, un'organizzazione deve essere preparata e in grado di adattarsi ai cambiamenti che sono richiesti prima, durante e dopo ogni avversità. Inoltre, se l'evento dovesse provocare impatti negativi, dovrebbe tentare di prevenirlo o di imparare dall'evento come riallinearsi o addirittura reinventarsi totalmente, per meglio adattarsi al nuovo contesto. Ciò che è stato trattato finora potrà apparire ancor più chiaramente a chi avrà voglia di leggere l'intero ANSI/ASIS SPC.1-2009. Lo troverà esaustivo per affrontare e rispondere ad ogni tipo di evento distruttivo, sia intenzionale che non intenzionale o di tipo naturale. [2]

Giunti a questo punto mi preme precisare che uno standard da solo, qualunque esso sia, non può garantire il risultato che lo stesso si prefigge. Sono necessarie doti manageriali e capacità organizzative adeguate al risultato che si vuole raggiungere. Una volta ancora, quindi, la componente umana prevale su quella procedurale. Non è possibile, per nessuna organizzazione, riuscire ad ottenere dei risultati senza la capacità manageriale di chi la conduce. Questo vale anche per la Resilienza Organizzativa. Ciò che uno standard può aiutare a realizzare è quello di adottare un modello organizzativo già sperimentato e un management system collaudato. Tutto il resto dipende dalla componente umana, sia del management che dei soggetti attivi.

Più avanti cercheremo anche di esplorare questi aspetti umani. Alla prossima puntata.

[2] Solo per dare un'idea, già a pagina 2 dello standard è precisato: "questo Standard consente ad un'organizzazione di: a) sviluppare una *policy* di prevenzione, preparazione e risposta/continuità/recovery; b) stabilire gli obiettivi, procedure e processi per raggiungere gli impegni fissati per *policy*;c) assicurare competenza, consapevolezza e formazione (necessaria per); d) impostare parametri per misurare le prestazioni e dimostrare la validità delle scelte; e) adottare azioni necessarie per migliorare le prestazioni; f) dimostrare la conformità del sistema ai requisiti di questo standard; g) stabilire e applicare un processo per un costante miglioramento. L'allegato A alle pp- 18-40 , che di fatto è la Guida per l'utilizzo dello standard, copre maggiori dettagli: ne parleremo in un numero successivo.

Alessandro Lega (*)

La Resilienza delle organizzazioni, puntata # 3

Per completare lo scenario che abbiamo trattato nel numero precedente riguardo il primo standard rilasciato nel 2009 negli Stati Uniti (ANSI/ASIS SPC.1-2009), dobbiamo parlare anche del suo logico proseguimento che è uscito nel 2012 con il nome di *Maturity Model for the Phased Implementation of the Organizational Resilience Management System* (ANSI/ASIS SPC.4-2012).
Come il titolo fa intravvedere, lo scopo di questo standard è quello di fornire una guida per l'adozione graduale di soluzioni organizzative a sostegno della Resilienza Organizzativa, in base ai diversi livelli di maturità raggiunti dall'organizzazione stessa. E' quindi una sorta di traccia, seguendo la quale un'organizzazione può progredire nella completa adozione del più alto livello di Resilienza Organizzativa, prevedendo stadi intermedi prima di arrivare a "full speed". Una modalità quindi in grado di procedere per tappe nell'adozione dell'ANSI/ASIS SPC.1-2009, evitando costi eccessivi e assicurando la possibilità di verificare il progressivo livello di maturità raggiunto.

L'ANSI/ASIS SPC.4-2012 propone sei fasi da completarsi in sequenza, suggerendo di verificare il corretto passaggio per gradi da una fase all'altra. Vediamo brevemente come si susseguono le sei fasi proposte. La **fase uno** corrisponde ad uno stato di pre-consapevolezza, in cui l'organizzazione si trova prima di valutare come intraprendere il cammino graduale. Nella **fase due**, con approccio al Progetto, l'organizzazione inizia ad avere consapevolezza ed il management comincia a definire gli obiettivi. Oltre agli obiettivi, nella fase due verranno definiti i ruoli, le responsabilità, il budget, il metodo di misurazione dei progressi. Già in questa fase è essenziale che il top management fornisca il pieno supporto al Project Leader individuando, dove necessario, il training e l'expertise necessari per sostenere il progetto. Nella **fase tre**, con approccio al Programma, l'attenzione si concentra su aspetti specifici in grado di creare le condizioni di successo e

(*) CPP

di aumentata consapevolezza. Questa fase fornisce al Program Manager l'opportunità di estendere il progetto coinvolgendo un numero maggiore di soggetti. Allo stesso tempo i vari soggetti contribuiscono all'individuazione di potenziali rischi che potrebbero ridurre la Resilienza Organizzativa e le relative probabilità che ciò avvenga. La **fase quattro**, con approccio al Sistema, vede l'inizio della messa insieme dei vari pezzi. Il top management è attivamente coinvolto nell'impostazione del management system.

I diversi attori coinvolti iniziano a testare le principali parti dello standard e le evidenze emerse nel corso degli audit vengono utilizzati per rinforzare i punti deboli del processo. La **fase cinque**, con approccio al Management System, coincide con la completa adozione di un sistema di gestione. Gradualmente viene introdotta una cultura di resilienza organizzativa. I programmi di formazione e di awareness diventano argomenti di routine per le risorse umane. Nella **fase sei**, approccio al Management Olistico, si va oltre la compliance e allo standard, raggiungendo un livello totalmente integrato di management della Resilienza Organizzativa. La gestione della Resilienza e i principi di Management System si estendono a tutte le aree di business e a tutte le attività aziendali. A questo punto, in sei mosse, un'organizzazione di tipo "giovane" può raggiungere uno stato di "maturità" attraverso un percorso in grado di far realisticamente raggiungere il risultato desiderato. Lo standard indica questi passaggi come fosse un percorso simbolicamente sportivo: Fase uno, di pre-consapevolezza; Fase due, del Bronzo; Fase tre, dell'Argento; Fase quattro, dell'Oro; Fase cinque, del Platino; Fase sei, del Diamante.

Abbiamo visto come uno standard disegnato per raggiungere un alto livello di Resilienza Organizzativa possa essere adottato in modo progressivo tramite un altro standard attuativo. I due standard ANSI/ASIS che abbiamo commentato sono infatti complementari e devono essere visti come un tutt'uno: il primo indica cosa fare, mentre il secondo propone come fare ciò che il primo indica necessario per raggiungere un adeguato livello di Resilienza Organizzativa (R.O.).

Fin qui abbiamo parlato della vision Nord Americana circa la R.O., che si è sviluppata fra il 2009 e il 2012. Vediamo adesso cosa è avvenuto in Europa e più precisamente in Gran Bretagna, con la pubblicazione a novembre dell'anno passato del BS 65000:2014 da parte del British Standard Institute. Si deve dare atto che nelle 23 righe dell'introduzione di questo BS viene immediatamente dichiarata la finalità che si prefigge, anticipando che: la Resilienza Organizzativa è un obiettivo strategico per aiutare le organizzazioni a sopravvivere e a prosperare; un'organizzazione resiliente è in grado di adattarsi meglio, essere più competitiva, snella e robusta di quanto lo siano quelle meno resilienti; la Resilienza Organizzativa è la base per garantire la capacità di un'organizzazione di anticipare, prepararsi per rispondere e adattarsi a qualsiasi condizione, dagli eventi quotidiani ai cambiamenti più intensi, sia temporanei che permanenti; la Resilienza è un concetto relativo e dinamico e come tale un'organizzazione può solo essere più o meno resiliente.

Come risultato da raggiungere, la Resilienza è un obiettivo e non un'attività permanente o una condizione di stato. Un'organizzazione opera già in una potenziale e complessa rete di interazioni con altre organizzazioni, per cui è essenziale che la Resilienza non venga "costruita" solo all'interno di un'organizzazione ma che sia estesa anche a tutta la rete e sia presente nelle interazioni con le altre organizzazioni. Sono ancora più succinti i tre punti che descrivono lo scopo della BS 65000:2014: 1) rendere chiaro al Top Management la natura e lo scopo della Resilienza Organizzativa; 2) identificare i principali componenti della Resilienza Organizzativa per rendere possibile ad un'organizzazione di rivedere la propria resilienza nell'adottare e misurare i propri miglioramenti; 3) identificare e raccomandare buone pratiche già definite in altri standard esistenti e in alcune discipline. Tutto ciò viene rafforzato ulteriormente nella parte che parla dei principi che caratterizzano la Resilienza Organizzativa, aggiungendo che essa ha che fare con "disruption", "uncertainty and change" con un chiaro proposito, con una precisa coerenza e con un riferimento alle opportune risorse necessarie. Prosegue poi elencando i benefici che derivano dall'avere un'organizzazione resiliente, mettendo in evidenza: la competitività, la coerenza, l'efficienza e l'efficacia, la reputazione e la resilienza dell'intera società civile. A questi benefici abbina la necessità di considerare un certo numero di opportunità e di punti di domanda, fra i quali: a) comprendere quando il management deve entrare in azione; b) trovare il giusto compromesso fra costi e livello di resilienza; c) determinare un appropriato trade-off fra il controllo dei costi e il raggiungimento di un più alto livello di resilienza; d) identificare

quando adottare nuovi valori piuttosto che continuare con i comportamenti esistenti; e) risolvere i conflitti fra la necessità di mantenere riservate le informazioni fra competitor e la necessità di condividere informazioni per la resilienza quando si è in collaborazione con altri; f) identificare le limitazioni di tipo legale e normativo, così come per i codici volontari di comportamento adottati dai diversi settori, che possono limitare specifiche azioni a supporto della resilienza; g) concludendo che ciascuna organizzazione deve prendere le proprie decisioni riguardo questi punti in base alle tipologie di rischi e del loro relativo livello che si intenda raggiungere, oltre a decidere in base alla dichiarata volontà di quanto si voglia investire in resilienza. Una particolare attenzione viene posta nel descrivere i requisiti fondamentali richiesti per costruire una organizzazione resiliente. Fra questi emergono: aspetti generali relativi alle attitudini dell'organizzazione; Governance e Accountability, intesa quest'ultima come attitudine del management di farsi carico dei risultati (positivi o negativi); Leadership e Cultura, intesa come diffusione delle due dimensioni; visione comune e progettuale. Un punto importante è rappresentato da come la BS 65000:2014 inquadra le condizioni necessarie per costruire un'organizzazione resiliente: la Resilienza Organizzativa richiede l'abilità di prendere valide decisioni basate sulla comprensione di dove l'organizzazione sia posizionata, dove intende arrivare, il contesto in cui agisce, quale sia l'interesse dell'organizzazione e quali siano le risorse disponibili.

MAPPATURA DELLE FASI E MISURAZIONE DELLA RESILIENZA

Rimangono due aspetti da valutare per completare l'analisi della BS 65000. La prima è la mappatura delle sei fasi che ruotano intorno al nucleo centrale rappresentato da Governance e Accontability, Leadership e Cultura, Visione comune e progettuale. Tutto deve ruotare intorno ad un fulcro ben determinato. A conferma che la Resilienza Organizzativa richiede un approccio multi-culturale e multi-disciplinare, la BS 65000:2014 richiama oltre venti discipline che devono essere attivate con modalità coerenti. Fra queste richiama: asset management, risk management, reputation management, environment management, health&safety, fraud control, business continuity, ICT security, cyber security, change management, physical security, facility management, emergency management, crisis management, supply management, human resources management, financial control e quality management.

Il secondo aspetto riguarda le modalità per misurare la maturità e la resilienza di un'organizzazione che la BS 6500:2014 individua nei seguenti sei punti, che devono essere decisi dall'organizzazione: 1) cosa è necessario monitorare e misurare; 2) il metodo di monitoraggio, misurazione, analisi e valutazione per assicurare risultati validi; 3) come effettuare un assessment costante della resilienza; 4) individuare il limite entro il quale l'output delle misurazioni possa essere considerato accettabile; 5) con quali modalità le misurazioni e il monitoraggio potranno lavorare insieme a ciò che è già in essere per i processi già esistenti; 6) come devono essere analizzati e valutati i monitoraggi e le misurazioni dei risultati. Per quanto riguarda la classificazione del livello di maturità raggiunta da un'organizzazione, la BS 65000:2014, a differenza della ANSI/ASIS SPC.4-2012, non propone una classifica sportiva bensì un ranking di performance stabilendo che il livello 0 corrisponde ad un'organizzazione Immatura (Immature); il livello 1 ad un'organizzazione di Base (Basic); il livello 2 a quello di Gestita (Managed); il livello 4 a quello di Affermata (Established); il livello 5 a quello di Lanciata (Predictable); il livello 6 a quello di Ottimale (Optimazing). Pur non entrando in dettaglio su come arrivare ad ottenere i risultati attesi e con quali modalità poter procedere per step successivi, come invece fanno le due ANSI/ASIS SPC.1-2009 e SPC.4 2012, la BS 65000:2014 propone una serie di 24 domande divise in sei gruppi che corrispondono a ciascun settore della figura prima riportata, le cui risposte corrispondono ai punti rilevanti che vengono trattati nello standard. Non quindi una guida ma una sorta di "lista della spesa", con le indicazioni su come trovare le risposte alle 24 domande.

Si potrebbe quindi dire che i tre standard finora commentati (ANSI/ASIS SPC.1-2009, ANSI/ASIS SPC.4-2012 e BS 65000:2014) si integrano perfettamente, senza particolari conflitti fra di loro, aggiungendo che per ottenere un'organizzazione allineata con i più attuali criteri di Resilienza Organizzativa è forse necessario attingere dai tre standard indicati. Questa fra l'altro è una conclusione a cui sono arrivati, oltre a me, anche i guru Nord Americani ed Europei della Resilienza Organizzativa, di cui vorrei accennare nelle prossime puntate. Per il momento ci salutiamo qui; alla prossima puntata.

Marc H. Siegel(*)

Organizational Resilience: oltre il solito blablabla

All'ultima European Security Conference and Exibition (Francoforte, 29/31 marzo) Alessandro Lega ha incontrato alcuni "guru" della Resilienza Organizzativa per sentire la loro opinione. La prima persona interpellata è stata Marc Siegel, Commissioner, Global Standards Initiative ASIS International, European Bureau. Si parla infatti molto di Organizational Resilience, sono stati prodotti alcuni standard ed altri sono attesi nei prossimi anni, ma – ricorda Lega - Siegel ha una visione disincantata ma qualificata sull'argomento. Quali sono dunque i fondamentali su cui porre le basi dovendosi imbarcare in un'avventura organizzativa, quale è quella di cui qui si parla?

(*) Commissioner, Global Standards Initiative ASIS International, European Bureau

"Organizational resilience" è un'espressione talmente abusata da essersi ormai svuotata di contenuti. Dai programmi governativi agli enti di standardizzazione, fino al settore privato: resilienza organizzativa è la parola più in voga per promuovere progetti o servizi. Ironia del destino, in questo straparlare di organizational resilience si è perso uno dei fattori chiave per costruire la vera resilienza aziendale. Proprio quando infatti le aziende cominciano a realizzare che un approccio integrato, proattivo e multidisciplinare alla gestione dei rischi può generare efficienze, chi si occupa di specifiche discipline afferenti al rischio reclama la paternità di tale espressione per promuovere i propri servizi. Ebbene, è ora di uscire dal solito blablabla e di concentrarsi sulla costruzione di un'organizzazione che sia coesiva e resiliente. Questo significa focalizzarsi sui principi fondamentali di un buon sistema integrato di gestione aziendale e del rischio.

NIENTE APPROCCIO STANDARD

Qualunque attività è soggetta ad una serie di rischi ed incertezze. L'incertezza è uno stato le cui conseguenze sono ignote, indeterminate o indefinite, o laddove vi sia una carenza di informazione. Le conseguenze possono insomma essere sia positive che negative. Soggetti singoli, strutture aziendali e comunità devono decidere quale livello di rischio e incertezza intendono accettare e prendersi in carico per raggiungere i propri scopi ed obiettivi. Tali scopi possono includere obiettivi strategici a lungo o breve termine, obiettivi legati all'intera o a una sola parte dell'organizzazione e della sua catena del valore, ma anche questioni tattiche o operative a tutti i livelli aziendali. La gestione di tali rischi, pertanto, dipende dagli obiettivi della struttura, dalla sua voglia di rischiare o di cogliere un'opportunità o di minimizzare una possibile conseguenza negativa. E' quindi di tutta evidenza che non possa esistere formula univoca o approccio standardizzato in materia.

STOP AI SILOS

La resilienza diventa importante da integrare nel processo di gestione del rischio perché promuove e al contempo richiede una logica di estrema adattabilità e snellezza organizzativa. La resilienza enfatizza infatti la gestione del rischio, sia nella sua multi-dimensionalità che nella sua durata temporale. La resilienza si basa sul principio che la gestione del rischio debba accrescere la capacità di adattamento in un ecosistema in costante cambiamento. Pertanto, la resilienza valuta in che modo integrare pienamente una gestione del rischio olistica e proattiva all'interno di buone pratiche di gestione aziendale, particolarmente nei processi decisionali a lungo e breve termine. Non si tratta solo di far convergere varie discipline afferenti al rischio, ma di farlo nel contesto degli obiettivi strategici, operativi e tattici dell'organizzazione d'impresa. La resilienza enfatizza il fatto che le organizzazioni diano per assunto di operare costantemente in un contesto dinamico e incerto. La resilienza esige sia di far convergere le discipline afferenti al rischio, sia di eliminare i "silos" organizzativi, e quindi di raggiungere un piano coordinato di gestione del rischio per l'intera attività d'impresa.

UN'OPPORTUNITÀ DI BUSINESS

La resilienza non è qualcosa di nativo, di insito nell'organizzazione: la capacità di adattamento si sviluppa infatti con la maturazione dell'organizzazione stessa, si apprende da successi ed insuccessi, cresce assieme alle capacità di prendere decisioni e alla conoscenza e all'approfondimento dei fattori, interni ed esterni, che possono influire sulle performance aziendali. La resilienza nasce anche da relazioni di contorno, prospettive culturali e in genere dalla capacità dei singoli di affrontare stress e avversità. Pertanto, la resilienza è in funzione di una varietà di comportamenti, pensieri e azioni che possono essere appresi e sviluppati in qualunque momento. All'interno delle organizzazioni aziendali, la resilienza somiglia alla resilienza umana nel fatto di non rappresentare tanto una *caratteristica*, quanto piuttosto una *prospettiva* del vivere in costanza di rischio: le organizzazioni resilienti integrano infatti la gestione del rischio in tutti i loro processi decisionali. Dare per assunto che rischi ed incertezze esistano in ogni circostanza significa che i decisori possano adeguarsi alle negatività, attutire i colpi e rimettersi in sesto ma al contempo identificare e cogliere delle opportunità di business. Le strutture che coltivano una cultura di problem-solving accresceranno questa loro resilienza (abilità che si sviluppa maggiormente allorquando si riconosce che fronteggiare un'avversità non significa necessariamente o soltanto fare un passo indietro, bensì rappresenta una possibilità di conoscenza e quindi di adattabilità). La resilienza promuove un processo di gestione degli eventi

avversi, di conoscenza e di perseveranza utilizzando un approccio sistemico. Gestire un'azienda e i rischi cui essa è esposta non significa solo disporre di tutti gli elementi per una buona gestione, ma anche comprendere le molte relazioni che insistono tra tutti questi elementi. I problemi vanno infatti affrontati pensando anche agli scenari che si potrebbero profilare in futuro, anche in considerazione della direzione che l'azienda vuole prendere. E' quindi un processo proattivo e preventivo/predittivo, che mette in luce il fatto che adattarsi a livello organizzativo prima che un evento si manifesti può generare nuove efficienze. Pianificare una gestione del rischio in maniera integrata rispetto a tutti gli aspetti della gestione aziendale è del resto diverso dal semplice reagire ad eventi che si dovessero presentare. Tuttavia, le strategie di business e risk management riconoscono che non tutti i fattori di incertezza, e soprattutto i loro possibili risultati, possano essere identificati o quantificati, perciò le criticità degli assett, delle attività e dei servizi sono determinate per delle operazioni sostenibili. "Recuperare" (la famosa recovery) non significa solo rientrare alla normalità, ma considerare il nuovo contesto derivante dal diverso ambiente operativo e (ri)determinare i punti dove la struttura è meglio posizionata. Essere un'organizzazione resiliente significa saper sfruttare in maniera efficiente tutte le sue risorse: umane, tangibili e intangibili. E poiché qualsiasi realtà dispone di risorse limitate, comprendere il risk management nel contesto di queste limitazioni permette all'azienda di individuare prima i propri punti di forza e di fare meglio leva sugli stessi. L'approccio al "problem solving" deve poi considerare le dipendenze e le interdipendenze aziendali: le organizzazioni resilienti sviluppano una rete forte di relazioni con gli stakeholder, le altre realtà aziendali e la comunità. Attraverso queste relazioni l'azienda è in grado di individuare la propria collocazione in un quadro più ampio, può imparare osservando e condividendo informazioni e sa dove cercare quando serve aiuto. Le organizzazioni resilienti hanno tante risorse, e sanno bene che le relazioni con gli stakeholder sono quelle di gran lunga più importanti. Un'organizzazione resiliente deve quindi saper incoraggiare e motivare gli stakeholder a lavorare per il bene comune. Promuovere le abilità comunicative e le consultazioni è quindi essenziale per accrescere la resilienza perché il rischio è meglio gestito con continue consultazioni e comunicazioni bidirezionali con gli stakeholder. Un'organizzazione resiliente crea quindi meccanismi tali da supportare sia un flusso di informazioni top-down che bottom-up: abilitare tutti, a tutti i livelli organizzativi, ad essere ascoltati rafforza il senso di inclusione che porta poi alla condivisione di pensieri e di idee. Ciò alimenta la diffusione di quella cultura del rischio per la quale sia chi lo può generare, sia chi lo corre comprende di essere egli stesso portatore e manager del rischio stesso. Un migliore flusso di informazioni basato sul senso di inclusione a sua volta promuove un'assunzione di decisioni più informata. Sostenendo che l'innovazione continua, la creatività e l'acquisizione di informazioni e competenze sono valori "core" per l'azienda, le persone che in essa lavorano avranno un approccio proattivo alle problematiche, contribuendo esse stesse ad incrementare la capacità di adattamento dell'organizzazione. Nel contempo si costruirà un senso di governo della situazione capace di ingenerare negli operatori la sensazione di essere parte attiva della soluzione e non del problema.

UN PROCESSO EVOLUTIVO

Il cambiamento è una delle poche costanti del mondo. Ecco perché la resilienza e la capacità di adattamento

spostano la prospettiva della gestione del rischio intesa come mera disaster recovery ad una gerarchia diversa, composta da parole ed azioni come. anticipare, impedire, prevenire, proteggere, mitigare, rispondere e ricostruire. Questo implica una continua ed accurata situational awareness, con un particolare focus sul monitoraggio degli indicatori di cambiamento prima che l'evento si manifesti. Ma significa anche sviluppare strategie di gestione del rischio che permettano all'azienda di *adattarsi preventivamente*, quindi di essere preparata ad attutire i colpi, ad imparare dalle esperienze proprie ed altrui e ad evolvere in un'organizzazione sempre più forte. Essere resiliente non significa naturalmente che una realtà aziendale non possa mai subire le conseguenze di un evento avverso: significa però che possa essere meglio preparata per identificare, comprendere ed adattarsi al cambiamento richiesto. Perché la resilienza è un processo evolutivo. Riconoscere nuove possibilità ed opportunità non significa operare cambiamenti bruschi ed impulsivi: al contrario significa approcciare il problema con quell'equilibrio e quella misura che solo un'informazione accurata può offrire. In conclusione, la resilienza organizzativa deve saper guardare oltre l'analisi del rischio. Costruire resilienza significa quindi vedere l'inevitabilità di alcuni rischi ma creare il potenziale per aver comunque dei risultati positivi. Chi lavora in un'organizzazione resiliente deve chiedersi sempre quali cambiamenti può fare per rafforzare lui stesso l'azienda. Perché resilienza significa anche conoscere esattamente dove ci si trova per sapere poi quale direzione prendere, quindi significa comprendere le proprie debolezze e le minacce cui si è soggetti per poi costruire nuovi punti di forza e nuove opportunità.

Dai commenti di Marc Siegel pare avere la conferma che creare organizzazioni senza "silos" ed in grado di mettere tutti i soggetti interessati alla gestione dei rischi in contatto fra di loro sia la mossa vincente. "You're right" - conferma Siegel. Alla prossima puntata con nuovi guru e opinionisti!

Alessandro Lega

Allison Wylde(*)

Resilienza organizzativa: l'approccio accademico

Come era stato anticipato nel numero precedente, Alessandro Lega, in occasione del 2015 European Security Conference & Exhibition che si è tenuta a Francoforte ad inizio aprile, ha incontrato diversi professionisti e guru a livello mondiale che si occupano di Resilienza Organizzativa. Oltre al contributo che è stato già pubblicato nel numero di agosto, ci ha fatto avere l'opinione centrata su aspetti accademici che ha potuto discutere con Allison Wylde, senior lecturer at the Regent's University of London, su ciò che sta accadendo nel mondo accademico, in ambito Resilienza Organizzativa. Le conclusioni sembrano confermare ciò che era già emerso in precedenza.

(*) FRGS DIC (Imperial), membro della Commission on Standards and Governance di ASIS International, ha co-diretto l'ASIS/ANSI Security Management Standard on Pyhysical Asset Protection (2012). Le sue ricerche si concentrano sulle percezioni degli operatori della sicurezza nei processi di decision-making.
wyldea@regents.ac.uk.

Nel mondo professionale come in quello accademico, la resilienza è un tema assai gettonato. Basti pensare che una ricerca eseguita il 30 giugno 2015 inserendo la parola "resilienza" nel motore di ricerca accademico Google Scholar ha prodotto più di 1,14 milioni di articoli – 240mila dei quali relativi al solo 2015. In cosa si traduce, per i security manager, tutto questo interesse? Cosa possiamo imparare da questi studi? In che modo la conoscenza così acquisita può aiutarci a intervenire nei dibattiti in corso ai più alti livelli? In primo luogo, prenderemo in esame gli aspetti su cui c'è accordo e quelli sui quali ancora si discute quando si parla di resilienza – perché inevitabilmente, le divergenze di opinione non mancano. Cercheremo quindi di capire cosa significa, in concreto, il termine "resilienza" e, infine, esploreremo il modo in cui un pensiero resiliente può aiutare i professionisti della sicurezza a migliorare tanto le loro strategie ai massimi livelli quanto i loro strumenti tattici.

OPINIONI DIVERGENTI

Nel settore della sicurezza, il tema della resilienza ha provocato reazioni contrastanti tra i manager come tra i membri della comunità accademica. Se alcuni lo hanno subito fatto proprio, altri hanno storto il naso continuando a percorrere strade già battute – e altri ancora, del resto, potrebbero spingersi a rifiutare del tutto qualsiasi nuovo tema "caldo" come forma di resistenza al cambiamento *tout court*. Negli ambienti universitari molti accademici sostengono a gran voce il loro specifico punto di vista sulla resilienza, presentando i risultati delle loro ricerche a supporto delle tesi avanzate. Posizioni che esistono almeno in parte per via dell'esistenza di veri e propri "silos" accademici nei quali i docenti proteggono i loro "confini" con le loro ricerche e, spesso, anche con un loro linguaggio peculiare.

Quando ingegneri e ricercatori dell'IT parlano di resilienza potrebbero riferirsi a qualcosa di completamente diverso rispetto a quanto inteso dagli scienziati ambientalisti (parlo da ex scienziata di laboratorio). Nelle scienze cliniche e comportamentiste, ad esempio negli studi sulla prima infanzia, si riscontra una variabilità ancora maggiore nei punti di vista sulla resilienza. Nonostante questo, ogni accademico reclama l'assoluta correttezza del proprio approccio specialistico. Per fare un esempio, in occasione di una recente conferenza internazionale, numerosi e autorevoli professori di marketing si sono messi a discutere sul fatto che gli "standard" possano o meno essere "ammessi" nel mondo accademico (Egan, 2015). Cerchiamo ora di capire in modo più preciso che cosa si intende allora per resilienza; più avanti vedremo perché sia utile comprendere queste differenze di opinione.

DEFINIRE LA RESILIENZA

Un dizionario offre le seguenti definizioni di resilienza: l'atto del recuperare; elasticità; conservare la forma originaria dopo la compressione; energia assorbita dopo lo sforzo (OED, sito web, 2015). Nel campo della sicurezza, gran parte delle riflessioni sul tema si concentrano oggi sulla capacità di adattamento. Tuttavia, come la definizione dell'OED chiarisce molto bene, la resilienza è molto di più. Diamo dunque un'occhiata al mondo accademico per capire quali idee potremmo mutuarne. Nell'ingegneria come nell'IT, un aspetto della resilienza si riferisce alla "resistenza" di un componente, ovvero all'arco di tempo nel corso del quale esso è in grado di reggere un carico prima di cambiare stato o cedere. Nella scienza ambientalista, la resilienza è invece considerata mediante un approccio sistemico in base al quale si esamina il modo in cui singoli "agenti" (organismi, organizzazioni, ecosistemi o biosfere) rispondono a molteplici sistemi che interagiscono fra di loro allo stesso tempo. Il concetto di "capacità di carico" è invece utilizzato per illustrare la popolazione massima che un sistema può sopportare prima di sbilanciarsi. Si può ad esempio considerare il numero di predatori e prede presenti in un ecosistema: se ci sono troppi predatori, le prede avranno un serio problema. Ancora, se in un corso d'acqua la presenza di alghe diventa eccessiva, il risultato è un avvelenamento dei pesci causato dal troppo azoto. E così via.

UN APPROCCIO DIVERSO ALLA VALUTAZIONE DEL RISCHIO

Negli studi sulla prima infanzia ci si focalizza sul comportamento adattativo dei bambini a seguito di un trauma. Bisogna tuttavia considerare che l'adattamento è un processo graduale, che richiede tempo: tornando all'esempio dei predatori e delle alghe, è ovvio che prede e pesci possono scomparire prima di essere riusciti ad adattarsi alle nuove condizioni ambientali. Nel mutuare queste idee dal mondo accademico – mi riferisco in particolare alla resistenza, alla capacità, all'equilibrio e

all'adattamento – i manager della sicurezza potrebbero guardare con occhio diverso alla valutazione del rischio dei loro asset, domandandosi ad esempio quali, tra di essi, sono portatori di quelle qualità al massimo grado e quali al minimo: dove si riscontra la massima resistenza? Dove la minima adattabilità?

Se i manager riescono ad adottare un approccio pragmatico, allora possiamo dire di essere fortunati perché siamo nella posizione di individuare e scegliere teorie realmente utili nell'esercizio quotidiano delle pratiche di sicurezza. Pensare in modo sistemico può essere utile anche per il fatto che le moderne organizzazioni sono immerse in una fitta rete di "relazioni" con i vari partner del ciclo di approvvigionamenti e con i relativi paesi di appartenenza (ben più di uno nel caso delle multinazionali, ovviamente). Queste "relazioni" includono (solo per citare qualche esempio) le obbligazioni legali e contrattuali, le responsabilità legate all'ambiente e alla sostenibilità, gli interessi di chi detiene quote dell'avviamento… In un contesto del genere una concezione della resilienza intesa come "resistenza, capacità e adattamento" potrebbe essere utile.

DALLA TEORIA ALL'AZIONE

Similmente a quanto avviene in ambito militare, i manager della sicurezza hanno messo a punto, in modo sempre più sistematico, una dottrina, ovvero un insieme coerente e strutturato di strategie di alto livello, tattiche e strumenti operativi provati e testati per guidare le decisioni e le successive azioni. I precedenti articoli già apparsi in questa serie, il *Security Risk Management Body of Knowledge* (cfr. Talbot e Jakeman, 2009) e un insieme di standard *ad hoc* potrebbero contribuire alla pratica della resilienza (vedi, ad esempio, lo standard ASIS/ANSI SPC1:2009: Wylde 2014), offrendo al contempo un'ampia gamma di metodi ed esempi di buona pratica ripetutamente testati. La conoscenza e l'applicazione della resilienza può offrire ai manager un supporto all'analisi e al miglioramento delle strategie e delle operazioni di sicurezza. Con un adeguato livello di comprensione di un concetto potenzialmente complesso come quello della resilienza, i manager possono continuare a dimostrare non solo la propria maturità professionale, ma anche la credibilità e la competenza necessarie per accrescere il valore dell'azienda e – aspetto essenziale – continuare ad avere il pieno sostegno del top management.

CONTINUARE A CRESCERE

Scopo di questo contributo era illustrare come i manager della sicurezza di oggi si trovino in una posizione fortunata: essi hanno infatti la capacità di riconoscere come la resilienza possa attingere a una vasta gamma di punti di vista e idee, e possono scegliere l'approccio che meglio si adatta alle necessità della loro organizzazione. Certo, abbiamo visto come intorno al concetto di resilienza vi siano divergenze di opinione in ambito accademico, soprattutto rispetto ai concetti di resistenza, capacità e adattamento. Ma i manager della sicurezza possono comunque fare riferimento a pratiche già consolidate come quelle del *Security Risk Management Body of Knowledge* (Talbot e Jakeman, 2009), nonché ad associazioni di settore e a organismi di standardizzazione come ASIS International. Infine, i manager della sicurezza hanno l'opportunità di condividere tra loro e con partner di fiducia strategie, strumenti operativi e idee partecipando a conferenze e progetti accademici. In questo modo potremo tutti trarne beneficio, continuando a crescere come professionisti.

Grazie Allison per l'esposizione molto chiara e in qualche modo premonitrice, che sembra confermare come la materia potrebbe evolvere in modo costruttivo. Ancorché ci siano opinioni non ancora del tutto concordanti, sembra che riguardo la possibilità di poter adottare organizzazioni basate su modelli evoluti di Resilienza Organizzativa stia trovando d'accordo sia il mondo accademico che quello dei professionisti della security. Speriamo che anche il mondo imprenditoriale sia della stessa opinione. Lo scopriremo nella prossima puntata.

Alessandro Lega

Alessandro Lega (*)

Luxottica: la resilienza organizzativa nel DNA aziendale

Siamo arrivati alla sesta puntata di questo lungo percorso dedicato alla Resilienza Organizzativa. Le prime tre sono state dedicate a descrivere i vari aspetti che contraddistinguono i diversi dispositivi di standardizzazione resi disponibili nel corso degli ultimi sei anni. La si potrebbe anche definire una terna di articoli che descrivono il riferimento normativo internazionale. Non si è fatto cenno alle iniziative nazionali, molto limitate dobbiamo ammettere. Unica eccezione è stata la Prassi di Riferimento UNI PdR 6:2014, pubblicata da UNI nel gennaio 2014, con il titolo *Infrastrutture Critiche – Sistema di gestione della resilienza – Requisiti*, prassi che può essere di aiuto ad individuare i requisiti necessari per la resilienza delle infrastrutture critiche. Un approccio che può essere adottato anche per strutture complesse. Vediamo adesso qualche caso virtuoso, di sobria efficienza, che possa confermare la validità di quanto trattato nelle cinque puntate precedenti. Inizieremo con un caso nazionale, giusto per sfatare la perenne convinzione che il nostro Paese non sia ancora pronto per introdurre innovazione organizzativa.

(*) CPP

Il primo caso viene dal Veneto ed è un'azienda nota ormai in tutto il mondo: Luxottica. Un brand che in pochi anni si è affermato a livello globale e che raggruppa realtà che fino a poco tempo fa erano viste come concorrenti. Sicuramente il top management di Luxottica ha dovuto fare ricorso ad un tipo di Risk Management molto innovativo. Non a caso abbiamo scelto Luxottica come primo caso di Resilienza Organizzativa da analizzare: guardando questa realtà da vicino, si percepisce immediatamente che il concetto di resilienza fa parte del suo DNA. Anche se l'azienda è passata attraverso diverse fasi di evoluzione e al momento è ancora in fase di evoluzione organizzativa, si percepisce che il suo fondatore ha voluto porre attenzione ad uno sviluppo resiliente, fin dai tempi in cui il concetto di Resilienza Organizzativa non aveva ancora un'identità definita come sta avvenendo negli ultimi anni. Se fossimo davanti ad un sistema operativo software, diremmo che Luxottica è un esempio di versione 4.0 con modulo applicativo di Resilienza Organizzativa *embedded* nel suo *kernel*. Certamente ad accelerare il processo di Resilienza Organizzativa di Luxottica ha fortemente contribuito la costante acquisizione di nuovi brand e la crescita registrata nel corso degli anni. L'alternativa sarebbe stata altrimenti quella di fare un patchwork, incollando insieme le diverse culture aziendali man mano aggregate, senza riuscire a salvaguardare l'identità che il fondatore ha fortemente voluto. Forse è anche vero che oltre all'intuizione iniziale del suo fondatore, Leonardo Del Vecchio, l'azienda ha saputo fare delle scelte organizzative che tutt'oggi le permettono di proseguire in questo percorso con decisioni che vengono condivise dal suo Senior Management e dagli oltre 78.000 dipendenti distribuiti nel mondo. Per avere una visione più ravvicinata di questa realtà, abbiamo avuto l'occasione di parlare con il **Group Risk & Compliance Director di Luxottica, Stefano Orsini**.

DALL'INTEGRAZIONE ALLA RESILIENZA

Siamo andati a trovarlo nella nuova sede piazza Cadorna a Milano, dove si trova la struttura Corporate del Gruppo Luxottica. I pochi minuti di attesa nell'accogliente reception, gestita in modo tecnologicamente evoluto, fanno immediatamente capire il clima aziendale e il significato del termine *Luxotticans*, cioè coloro che lavorano in Luxottica. Se ne possono incontrare diversi di loro mentre si muovono all'interno di un ambiente molto friendly, e molti altri, anche se solo in modo virtuale. L'area di attesa visitatori è infatti corredata di display su cui si possono visionare i gioielli di famiglia: non solo i prodotti e i brand del Gruppo, ma anche le persone che ne fanno parte.

L'incontro con Stefano Orsini avviene nel suo ufficio al quinto piano: faccio subito notare che il clima di resilienza si percepisce fin dal primo momento in cui si entra in sede. Le prime osservazioni di Orsini confermano le mie impressioni: "questa Azienda, che ha radici manifatturiere, ha dovuto da subito attivare un'integrazione per far dialogare fra di loro le varie anime che la compongono. Non solo in termini di prodotto e di brand, di per sé già fortemente resilienti, ma coinvolgendo tutte le funzioni che la compongono. Dal Product & Operations, a R&D & Enginereering, alla Produzione, al Manufactoring, al Wholesale, al Retail Sales (7000 punti vendita nel mondo). Il modello organizzativo vede il Consiglio di Amministrazione impegnato a definire la *Governance*, compresa la gestione del rischio; le funzioni di Controllo sono invece impegnate nel garantire l'*Execution* mentre Operations, Risorse Umane, e IT department sono coinvolte nel *Delivery*. Questo ha richiesto l'adozione di un approccio culturale capace di amalgamare le varie culture che si sono integrate nel tempo."

Fin qui si potrebbe commentare che Luxottica sia stata capace di far convergere le varie funzioni verso un'organizzazione integrata. Da qui a poter ottenere il risultato di una maggiore resilienza verrebbe da pensare che sia intervenuta qualche altra circostanza favorevole. Cosa? Pronta la risposta di Stefano Orsini. "Nel 2009 l'azienda ha deciso di costituire il department Risk & Compliance, affidandogli compiti specifici che includono il Risk Management, la Compliance, la Security e la protezione della Intellectual Propriety. Il compito affidato a questo nuovo department, che oggi conta circa 20 persone, è stato quello di avviare un'analisi dei rischi a 360 gradi individuando tutte le possibili minacce alla resilienza del Gruppo. In particolare è stata posta la massima attenzione alle capacità produttive *in house*, creando una Supply Chain in grado di intervenire in caso di *disaster*. Questa è una delle situazioni costantemente monitorate, sotto la G*overnance* del Comitato di Controllo dei Rischi che è sotto la diretta conduzione dell'Amministratore Delegato, a cui il Risk & Compliace Director riporta direttamente".

Si può dunque cominciare ad individuare i motivi che

fanno di Luxottica un'azienda di successo: azienda corta, visione imprenditoriale, forte leadership, forte identità e spirito di appartenenza, consapevolezza che una geografia così complessa non poteva ricorrere ad un modello tradizionale di Comando & Controllo. La soluzione poteva passare attraverso un processo di empowerment e di autonomia operativa. Due orientamenti confermati anche dalla scelta di separare il budget del department Risk & Compliance da quello del resto dell'azienda. Una scelta certamente strategica, in grado di non far correre il rischio di far andare in apnea una funzione che deve mantenere costante attenzione al processo di Resilienza, anche nel caso in cui l'intero Gruppo dovesse avere qualche defiance.

CAPITALE UMANO

Abbiamo quindi chiesto a Stefano Orsini quale sia il driver che permette a Luxottica di contare sull'intera struttura per garantirsi un alto livello di Resilienza. Ecco la risposta: "Luxottica ha adottato da tempo una cultura che è incentrata sulla valorizzazione dei dipendenti e sul loro pieno coinvolgimento, nel rispetto di caratteristiche e valori positivi che da sempre guidano l'azione dell'azienda. Il turnover, salvo in Cina, è attualmente molto basso, per cui gli interventi in grado di influenzare la cultura aziendale mantengono il loro effetto per una durata significativa". Sono considerazioni certamente importanti, ma forse non sufficienti per garantire un costante impegno a sostenere un alto livello di Resilienza. Inevitabile la domanda a Orsini: what else? Immediata e convinta la risposta: "Luxottica ha da sempre deciso di mantenere un ambiente il meno formale possibile per garantire una forte condivisione e partecipazione dei collaboratori, assicurando la massima attenzione al futuro, coinvolgendo le funzioni di staff (compreso il Department Risk & Compliance) in un ruolo di consulenza, a supporto delle altre funzioni aziendali, e incentivando coloro che sono coinvolti nei processi di Risk Management in base ai risultati ottenuti nel breve, medio e lungo termine. Tutto questo tenendo ben presente la necessità di mantenere alta la vocazione globale e non solo quella nazionale. D'altra parte la distribuzione geografica dell'azienda (oltre 42.000 collaboratori nel Nord America, dove Luxottica è leader del settore *eyewear*, circa 10.000 in Italia, oltre 17.000 nella regione Asia-Pacifico) non potrebbe garantirsi un alto livello di Resilienza se non ci fossero due condizioni indispensabili: un efficace processo di ricognizione dei rischi abbinato ad un forte *commitment* del management e dei collaboratori".

STANDARD? BUON SENSO

Avviandoci a salutarlo, abbiamo posto un'ultima domanda ad Orsini: qual è lo standard di riferimento che Luxottica ha adottato negli anni per dare supporto ai propri processi di Resilienza? Quello di ASIS International? Quello di BSI? Altri? Risposta molto concisa e chiara: "Nessun particolare standard. Solo tanto buon senso, adozione di *best practices* e forte intuito del top management. Avevamo inizialmente ipotizzato di conseguire alcune delle certificazioni relative alla Resilienza e al Risk Management, ma poi non le abbiamo ritenute necessarie". Lo salutiamo con la promessa di tornare a trovarlo fra qualche tempo. E' certamente un esempio da seguire con attenzione. Nella prossima puntata vedremo qualche altro caso che possa farci capire meglio come la Organizational Resilience si stia affermando, anche nel Public Sector.

ETHOSACADEMY

INFORMARE E FORMARE

FORMAZIONE IN MATERIA DI SECURITY E SAFETY

Una **scuola di formazione** che rappresenta uno dei più validi punti di riferimento per la formazione e l'aggiornamento di professionisti, uomini d'azienda, pubblica amministrazione.

media partner

a&S ITALY
Tecnologie e soluzioni per la sicurezza professionale

secsolution
security online magazine

Ethos Media Group srl
Via Caduti di Amola, 31
40132 Bologna (Italy)
Tel. +39 051 0475136
Fax +39 039 3305841
academy@ethosmedia.it
www.academy.ethosmedia.it

CORSI ATTIVI

Progettare Sistemi Videosorveglianza IP
In collaborazione con Gazzoli Engineering

Privacy Officer e Consulente della Privacy nel settore Videosorveglianza
Consulenza scientifica e patrocinio a cura di Federprivacy

Videosorveglianza e Privacy 2016. Road show
Corso di aggiornamento sulle novità in tema di videosorveglianza e privacy

Norme CEI Sistemi antintrusione e antirapina
In collaborazione con Gazzoli Engineering

Vendere sicurezza: come migliorare e sviluppare il processo di vendita

Obblighi, responsabilità civile e penale per gli operatori del settore Videosorveglianza

Analisi del Mercato per lo Sviluppo delle Vendite
In collaborazione con Galasso Consulting

Il Pensiero Laterale e i 6 cappelli per pensare
In collaborazione con Galasso Consulting

Il D. Lgs. 231/01: da Obbligatorietà ad Opportunità
In collaborazione con Galasso Consulting