ETICA A BRACCETTO CON SICUREZZA

di Clelia Pizzalli[1]

- *L'industria ha generalmente espresso per prima attenzione al tema sicurezza nell'ambito degli ambienti di lavoro, ancorché agendo non sempre "motu proprio", bensì troppo spesso in ottemperanza ai disposti legislativi. Come sta evolvendo, invece, il mondo della finanza in tema di "sicurezza"?*

- *Un'azienda non potrà crescere contando su spinte motivazionali tese a sviluppare serenamente le potenzialità, le aspirazioni e l'energia creativa delle persone, senza prima aver costruito un modo di lavorare realmente sicuro.*

Sicurezza: moda o bisogno?

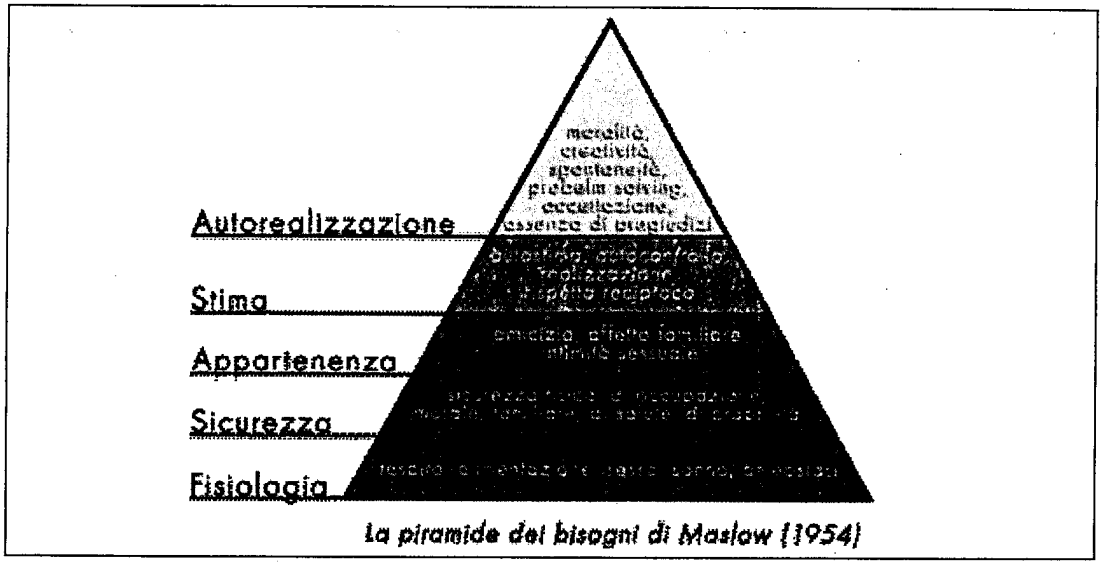
Cosa sta portando i giornali ed i notiziari ad occupare buona parte del loro spazio con eventi riconducibili alla sicurezza? Perché la sicurezza pare essere così di moda da essere citata, evocata ed esibita costantemente?
Probabilmente la sicurezza segue un po' la dinamica comunicativa dei valori: si sente il bisogno di parlarne molto quando si praticano poco.
Quando, infatti, la sicurezza era in testa alle priorità dei singoli Stati, non la si vedeva e si faceva dimenticare.

Analizzando questo tipo di notizie, ci accorgiamo, però, che sarebbe più corretto parlare di "insicurezza": nucleare (Fukushima), idrogeologica (Veneto), sismica (L'Aquila), insicurezza degli archivi di dati (Sony-PlayStatioNetwork, trafugati i dati di 77 milioni di utenti), dei PC (virus Zeus, ha già infettato 75.000 sistemi in 196 paesi, 2500 organizzazioni e rubato 68.000 informazioni), sociale (criminalità, terrorismo) e sul lavoro (Thyssen).
Le parole, però, creano la realtà, così se sostituissimo la parola "sicurezza" con quella più vera di "insicurezza" crescerebbe in noi un senso di spaventata precarietà che comprometterebbe i nostri più normali comportamenti.

Questa reazione difensiva è ben spiegata dalla piramide dei bisogni di Maslow che ha alla sua base i bisogni fisiologici (fame, sete, riposo, sessualità) ed i bisogni di sicurezza al livello immediatamente superiore.
I bisogni più evoluti (affetto, stima, autorealizzazione) li troviamo nei tre livelli più alti. Nessun bisogno superiore sarà soddisfatto se prima non risultano appa-

(1) Un ringraziamento particolare ai colleghi del Banco Popolare Marcello Anelli, Ivan Bruschi (Direzione Sicurezza) e Giancarlo Butti (Direzione Audit) per il materiale che mi hanno messo a disposizione.

gati i bisogni dei livelli inferiori.



La piramide dei bisogni di Maslow (1954)

Questo vale anche per le organizzazioni più complesse. Un'azienda, ad esempio, non potrà crescere contando su spinte motivazionali tese a sviluppare serenamente le potenzialità, le aspirazioni e l'energia creativa delle persone, senza prima aver costruito un modo di lavorare realmente sicuro.

La sicurezza, tuttavia, a differenza dei bisogni primari, poggia su una modalità gestionale particolare. Si perde molto lontano nel tempo quel patto sociale con il quale l'individuo ha delegato alla sua tribù prima, ed al suo Stato oggi, i compiti di garanzia della propria sicurezza individuale. Questo bisogno è sempre presente e tende a ripresentarsi prepotentemente tra le smagliature di una organizzazione sociale inefficiente: persone tranquille, qualora vengano attaccate, riscoprono ataviche reazioni istintuali e realizzano "adrenaliniche" aggressioni degne delle caverne primordiali.

La sicurezza richiama prepotentemente anche il concetto di legalità e di comportamento etico, che, pur differenziato nelle diverse declinazioni religiose o filosofiche, porta con sé un sentire comune di valori condivisi, l'osservanza dei quali garantisce e trasmette un clima di diffusa sicurezza, rispetto degli altri e benessere generalizzato.

L'industria ha generalmente espresso per prima attenzione al tema sicurezza nell'ambito degli ambienti di lavoro, ancorché agendo difficilmente "motu proprio", bensì troppo spesso solo in ottemperanza ai disposti legislativi. E il nostro mondo "finanziario"? Come si sta evolvendo sugli svariati temi legati al concetto di "sicurezza"?

Sicurezza fisica e informatica

In ambito bancario l'attenzione alle dinamiche di filiale, ove in generale il sistema registra una diminuzione del fenomeno delle rapine e di attacchi ai bancomat, è basilare per individuare e migliorare nel continuo sistemi di difesa quali ad esempio "cash in-out", sistemi di videosorveglianza e sistemi di anticamuffamento.

Come conseguenza di quanto sopra, si rileva uno spostamento dell'interesse delle bande criminali, orientato ora verso la clonazione delle carte, attività, per loro, meno rischiosa e più redditizia. La tempestiva attività di sostituzione di carte clonate, o sospette tali, aiuta a contenere perdite potenziali ingenti.

Un ulteriore incremento si registra sull'uso delle false identità, utilizzando documenti falsi o sottraendo credenziali e password per accedere, via web, ai patrimoni dei clienti. L'adozione di sistemi di controllo sempre più sofisticati e l'introduzione di dispositivi che generano password mono uso (c.d. "*token*") possono aiutare a comprimere questo fenomeno.

I tentativi di introdurre virus o codici malevoli sulle reti intranet tramite e-mail rimane una costante. Da anni c'è chi sostiene che la posta elettronica è morta a causa soprattutto dell'abuso che la gente ne fa; l'avvento dei *social network*, dei software di *instant messaging* ed il costante utilizzo degli sms possono far pensare che effettivamente la fine sia prossima. Ma la realtà dei numeri dice l'esatto opposto: nel mondo si è passati da 50 miliardi di e-mail spedite nel 2006 a 300 miliardi nel 2010; nel 2009 le caselle attive nel nostro Paese erano più di 56 milioni!

Ecco come possiamo pertanto difenderci dagli attacchi informatici: l'utilizzo di specifici strumenti denominati "*firewall*" ad elevata sofisticazione può arrivare a filtrare oltre il 90% delle mail in entrata. Un esempio numerico: nel Gruppo Banco Popolare le mail che i dipendenti leggono sulla propria casella personale rappresentano il 7% ca di quelle indirizzate all'intero Gruppo. In un anno vengono inoltrate all'utente 14 milioni di mail a fronte di 205 milioni pervenute. La configurazione e gestione dei *firewall* è un'attività specialistica che richiede personale qualificato. Nelle situazioni di maggiore criticità è opportuno avvalersi di servizi che garantiscono il costante monitoraggio dei *firewall*, al fine di individuare tempestivamente situazioni particolarmente critiche.

Le prove di evacuazione ed i continui test di continuità operativa garantiscono una sicura garanzia a fronte di disastri improvvisi. Chi non si è stupito vedendo le immagini dell'ordinata e ripetutamente "allenata" evacuazione durante il terremoto in Giappone? Può essere interessante sapere che la riflessione in questo

campo si sta sviluppando verso concetti di "*social continuity*" secondo la quale un'azienda preparata a gestire un'emergenza in un contesto sociale impreparato non è garantita in nulla. Ponetevi questa domanda: in caso di disastro grave (inondazione, terremoto) il vostro primo pensiero (e conseguentemente la vostra prima azione) andrà al lavoro del vostro ufficio od alla scuola dove stanno giocando e studiando i vostri figli? Non è forse vero che solo quando saprete che i vostri figli sono al sicuro comincerete ad occuparvi dei problemi della vostra azienda?

Sicurezza morale, familiare, di salute, di proprietà

La società in cui viviamo è certamente complessa: offre molte possibilità di aumentare le nostre conoscenze, di viaggiare, di conoscere persone e vivere esperienze diverse. La crescita del benessere economico è in generale positiva, ma, per mantenere l'attuale stile di vita, ci sottoponiamo spesso a notevoli sforzi fisici e mentali e ci può capitare di sacrificare in parte la nostra salute e le qualità dei nostri rapporti interpersonali.
Il mondo del lavoro nei Paesi industrializzati, in particolare, è sempre più caratterizzato da ridotta stabilità e crescente carico di lavoro, elevate richieste di flessibilità, di intraprendenza, di complessità di pensiero. Tutto questo comporta dei costi umani elevati: si osserva che le malattie considerate emergenti quali lo stress, la depressione o l'ansia, nonché la violenza sul luogo di lavoro, le molestie e l'intimidazione rappresentano quasi il 20% dei problemi di salute legati al lavoro: stiamo parlando di iniziative volte a fornire "sostegno della persona", ovvero supporto per la soluzione di specifiche situazioni di disagio individuali.

Già dai primi anni '80, negli USA, si sono sviluppate metodologie per aumentare le capacità delle aziende di far fronte alla complessità della società industrializzata e del mercato del lavoro con l'obiettivo di migliorare il benessere in azienda a tutti i dipendenti ed in particolare a coloro che sono in situazione di difficoltà o di malattia. Ora anche in Europa si stanno sviluppando esperienze in tal senso. Accanto alle forme tradizionali di assistenza, l'attenzione delle aziende si sta focalizzando su nuovi ambiti volti a permettere una maggior sicurezza morale nei propri dipendenti. Gli ambiti possono essere i più svariati:

- consulenza e supporto ai dipendenti per l'approfondimento di problematiche che influiscono sul benessere organizzativo (disabilità, dipendenza da sostanze, depressione, etc.);

- sostegno ai dipendenti che si trovano in situazione di disagio/difficoltà con ripercussioni negative sulla vita lavorativa;

- attivazione dei collegamenti con i servizi del territorio;

- consulenza ai dipendenti che hanno una certificazione di invalidità per un miglior abbinamento tra capacità e mansione;

- consulenza per migliorare l'inserimento lavorativo delle persone con disabilità, difficoltà, disagio.

Non necessariamente l'azienda su questi argomenti mette a disposizione specialisti, quali ad esempio psicoterapeuti: si offre al dipendente uno spazio d'ascolto per l'approfondimento della situazione di disagio e l'individuazione di un percorso di miglioramento della situazione personale e lavorativa.

Identificazione dei rischi e quantificazione dei costi

Nel suo libro "Sicurezza Totale"[2], Giancarlo Butti parte dalla necessità di protezione di tutti i beni aziendali: ogni bene ("*Asset*"), sia esso materiale, immateriale o rappresentato dal personale, è esposto ad uno specifico pericolo o minaccia. Una volta identificati gli *Asset* aziendali, sotto la voce "La gestione del rischio" viene suggerito un percorso per analizzare rischi, minacce, vulnerabilità, etc. Di seguito alcuni punti "salienti":

- valutare la possibile correlazione fra diversi *Asset*: un bene fisico può contenere un altro bene fisico, come un edificio che contiene al suo interno i vari locali e questi altri *Asset* aziendali, quali ad esempio le attrezzature. Nel caso di danno all'edificio, derivante ad esempio da un terremoto, si avranno ripercussioni anche sugli *Asset* in esso contenuti. Ma un bene fisico contiene anche beni immateriali e risorse umane rappresentate dal personale. Da qui la necessità di analisi delle correlazioni possibili;

- valutare la possibile correlazione fra rischi diretti, indiretti e consequenziali: la rottura di un disco fisso (rischio diretto) può portare alla perdita delle informazioni in esso contenute o all'indisponibilità del server che utilizza quel disco (rischio indiretto); quest'ultima può portare alla mancata erogazione di un servizio esterno, che può portare a sua volta alla perdita di un cliente, alla perdita di immagine aziendale, ad un contenzioso, etc. (rischi consequenziali);

- abbinare la correlazione dei rischi alla correlazione degli *Asset* per procedere con l'analisi dei rischi, che può conseguentemente essere particolarmente

(2) Edizioni Iter, 2011

complessa. Ogni azienda dovrà pertanto valutare quale sia il corretto livello di dettaglio da adottare; l'aggregazione di categorie di *Asset* fra loro omogenei è un modo per semplificare molto l'analisi dei rischi;

- analizzare i tipi di minacce, ovvero quell'azione volontaria, involontaria o l'evento accidentale che, sfruttando una vulnerabilità, provoca un danno. Le minacce possono essere variamente classificate e declinate; un esempio di classificazione può essere la suddivisione tra minacce ambientali (meteorologiche, sismiche, biologiche quali malattie o epidemie, etc), industriali (incendi, polveri, etc), guasti (ai sistemi informativi piuttosto che agli impianti) e comportamentali (furti, frodi, disobbedienza, scioperi, etc);

- analizzare le vulnerabilità caratteristiche di ogni bene, da ricondurre essenzialmente a carenze (ovvero mancanza di qualcosa) ed errori. Tra le carenze possiamo identificare quelle organizzative (mancanza di *policy*, mancata definizione dei ruoli, mancata identificazione del valore delle risorse, mancata definizione dei controlli e del processo di gestione degli stessi, etc) ovvero quelle nelle risorse umane (mancanza di procedure per la selezione e valutazione del personale, mancata gestione delle risorse umane e delle loro aspettative, mancato monitoraggio del clima aziendale, etc). La presenza di carenze può portare ad errori involontari oppure ad azioni volontarie contro l'azienda stessa.

Una volta determinati i rischi e gli elementi critici, ogni impresa è costretta (e sempre più lo sarà in futuro) a quantificare i costi derivanti da violazioni della sicurezza, non limitandosi alla mera valorizzazione monetaria di un *Asset*, bensì valorizzando anche il reale impatto che la distruzione di un Asset può provocare sul business aziendale. Senza un metodo coerente e sistematico questa attività diventa difficile. A questo proposito, alcuni propongono una tripartizione dei costi connessi:

- diretti: gli effettivi danni causati (ad es. costo del disco in caso di distruzione di un disco fisso);

- indiretti: i costi di ripristino (ad es. il costo sostenuto per l'intervento tecnico di sostituzione, ovvero il costo di ripristino di dati, applicazioni o configurazioni);

- consequenziali: i costi legati alle conseguenze (ad es. mancato guadagno temporaneo per cessazione del servizio, rimborso a clienti, spese legali per il ripristino dell'immagine aziendale, mancato guadagno per perdita di clienti ovvero perdita di quota di mercato).

Un'attenta analisi di valorizzazione è imprescindibile per permettere una corretta valutazione dei costi-benefici delle possibili contromisure che possono essere attivate per ridurre sia la probabilità di accadimento di un evento dannoso, sia l'impatto dell'evento stesso.

Conclusioni

Occorre non dimenticarsi che una continua formazione è la miglior garanzia di sicurezza. La legge costringe anche le aziende a basso rischio ad intensificare la formazione sulla sicurezza, perché il legislatore sa che per introdurre un cambiamento sociale evidente bisogna transitare dalla scuola e dal mondo del lavoro. Educati gli studenti ed i lavoratori, è il livello culturale di un intero Paese che cresce.

La cultura ed i comportamenti etici sono, però, patrimonio e libera decisione dell'individuo. A ciascuno di noi, quindi, resta il piacevole compito di alimentare costantemente la cultura della sicurezza per fare, così, il miglior servizio a noi stessi, alla nostra azienda, al nostro Paese ed ai nostri figli.