

BANCASICURA[®] 98

VIII° Convegno nazionale sulla sicurezza nelle Banche

Bologna, 12-13 febbraio 1998

Quartiere fieristico

LA VALUTAZIONE DEL RISCHIO CRIMINOSO NELLE BANCHE

<i>A. Marcello</i>	2
<i>L. Napodano</i>	4

© 1998 **A.I.PRO.S.** ASSOCIAZIONE ITALIANA PROFESSIONISTI DELLA SICUREZZA

Testi, relazioni ed immagini sono riproducibili solo dietro autorizzazione dell'A.I.PRO.S

LA VALUTAZIONE DEL RISCHIO CRIMINOSO NELLE BANCHE

DOTT. ANGELO MARCELLO

Consulente di sicurezza

Presidente Onorario A.I.PRO.S. Associazione Italiana Professionisti della Sicurezza

Seguendo un approccio di tipo quantitativo e razionale dei concetti di rischio e di sicurezza, indenni da ipoteche di tipo psicologico, nella prima parte del seminario è stato presentato uno schema operativo, detto "matrice dei rischi", ai fini della determinazione dei valori di riferimento da tener presenti in fase iniziale del processo di valutazione dell'esposizione di un'azienda al rischio di origine criminosa.

Rilevato che le componenti del rischio subiscono variazioni cronologiche e topologiche di non trascurabile grandezza, è stato suggerito l'utilizzo di una seconda matrice dei rischi, che tenga conto delle misure massime e minime che le due variabili indipendenti possono assumere nel tempo e nello spazio, si da valutare con ragionevole approssimazione i limiti minimo e massimo dell'entità del rischio globale di azienda dal tipo di eventi dannosi in rassegna.

E' stato quindi rappresentato un metodo grafico di esposizione del rischio globale da tale eventi, sottolineando come, nella sua delimitazione, intervengano criteri non solo obiettivi di tipo statistico e contabile, ma anche fattori soggettivi derivanti dall'età media del management, dalla misura accettata della trasferibilità sui costi delle perdite derivanti dal verificarsi degli eventi stessi, nonché dalla politica aziendale dei prezzi di vendita e degli ammortamenti.

Operata la distinzione fra rischi commensurabili ed incommensurabili, economici, etici, d'immagine ecc., è stato mostrato come dall'entità del singolo rischio sia possibile inferire il tipo di criminale che può porlo in essere, e quindi la natura ed intensità delle difese che possono predisporre, giungendo alla conclusione che l'esistenza di rischi che l'azienda non può accollarsi come costi eventuali della sua attività imprenditoriale postula la formulazione di strategie e tattiche per il fronteggiamento di essi.

*Tali strategie di fronteggiamento si riassumono nella **elusione** dei singoli rischi, nella **traslazione** di essi su altri soggetti, nella **repressione**, ad opera di proprie risorse o delle Forze dell'Ordine, ed infine nella **prevenzione** attraverso il ricorso ad apposite misure fisiche, umane e procedurali.*

*E' stata tentata una definizione provvisoria di **sicurezza** come una mera situazione di fatto, in cui più misure elementari vengono poste insieme al fine di minimizzare od annullare la misura del singolo rischio criminoso.*

Ciascuna di tali misure elementari si compone inevitabilmente di tre fattori di diversa natura, uno dei quali è l'essere umano, un secondo è uno strumento fisico attivo od inerte, ed un terzo è il fattore procedurale, inteso come norma dei comportamenti che l'essere umano, mediante l'uso degli strumenti e mezzi fisici a sua disposizione, deve tenere per raggiungere lo scopo della singola misura di prevenzione che esso compone.

*Essendo la misura dell'efficacia di ciascuna componente da considerarsi misurata in termini di sua **attendibilità**, e quindi di probabilità che essa operi nel modo atteso al verificarsi del singolo evento dannoso, la misura dell'efficacia composta della singola misura elementare di sicurezza viene ad essere pari (teorema di Bayes) al prodotto lineare delle misure della probabilità di funzionamento delle tre componenti, e quindi a situarsi fra lo zero (se anche una sola delle componenti ha efficacia nulla) e l'unità (quando tutte e tre esse hanno la misura massima pari alla certezza assoluta di funzionamento).*

Rammentata l'esistenza di un assunto che vuole che l'efficacia di un sistema è sempre maggiore della somma delle misure dell'efficacia delle sue componenti, si è pervenuti alla modifica dell'espressione che descrive la sicurezza ponendo, al denominatore della somma dei prodotti delle misure di sicurezza per l'efficacia di ciascuna di esse, l'espressione che riassume l'efficacia di sistema come prodotto dei margini di inefficacia di esse, spiegando che, se fra tutte le misure previste anche una sola opera al verificarsi dell'evento dannoso, quest'ultimo varrà egualmente sventato.

Sono stati quindi esposti alcuni esempi che provano la veridicità dell'assunto ed è stato infine operato lo spostamento del fattore di efficacia di sistema da denominatore dell'espressione della sicurezza a fattore dell'espressione del rischio, indicando quest'ultima, così modificata, come riassumendo la misura della "esposizione" o "vulnerabilità" globale della singola azienda agli eventi criminali censiti in fase iniziale di analisi. L'analisi delle esposizioni ai singoli rischi va a formare una seconda matrice, detta dei rischi residui, su cui occorre basare la ricerca delle misure integrative di sicurezza atte a ridurre ulteriormente l'entità individuale e globale.

Sulla base della considerazione che il rischio è in effetti una potenziale perdita economica (e non solo tale), è stata suggerita la necessità di utilizzare la matrice dei rischi residui come complesso dei valori di riferimento e confronto dei costi che le diverse scelte e strategie di fronteggiamento dei rischi comportano per l'azienda. In tal modo, in sede di confronto dei costi è possibile selezionare ed adottare solo quelle scelte che presentino un costo minore del rischio residuo da fronteggiare, in applicazione del criterio che se il costo del fronteggiamento del rischio è maggiore della misura di quest'ultimo, tanto vale correrlo.

I partecipanti sono stati invitati a non sottovalutare la difficoltà del metodo suggerito, ed ha raccomandato di intessere con la Direzione aziendale un dialogo basato su un comune linguaggio economico, che porti la Direzione a comprendere e condividere gli obiettivi del dipartimento Sicurezza Aziendale, ponendosi a sostegno di esso nell'avallare le scelte procedurali da questo proposte alla Direzione stessa.

ING. LUCIO NAPODANO

*Resp. Servizio Tecnico e Sicurezza e Servizio Prevenzione e Protezione
Banca Popolare dell'Irpinia*

La sicurezza è un argomento vastissimo, con il quale conviviamo nell'arco della nostra vita, quale che sia l'attività che stiamo svolgendo e persino nei momenti di relax o di riposo.

Per poterla progettare, realizzare e mantenere efficiente si è spesso obbligati a paralizzare e ridurre il problema ad entità che siano tecnicamente ed economicamente affrontabili. Per questo motivo si sente quasi sempre parlare di sicurezza in un settore (industria, casa, trasporti, sanità, scuola, servizi, ecc.) o di tecnologia, organizzazione e fattore umano, come si trattasse di argomenti isolati o isolabili.

Ma la realtà operativa è molto più complessa, a causa delle influenze reciproche e delle interazioni tra settori e componenti della sicurezza; perciò i costi che le aziende sopportano per attivare al proprio interno specifiche risorse assumono proporzioni sempre più rilevanti, rendendo indispensabili, per la loro valutazione, strumenti quali quelli esposti dal dott. Marcello nel suo intervento.

1. I CONCETTI DI SICUREZZA E RISCHIO

Sono state proposte numerosissime definizioni del termine *sicurezza*. Una delle più significative, per la sintetica concretezza che esprime, è quella secondo la quale essa è costituita da una "somma di misure efficaci"

$$S = \sum_i M_i \times E_i$$

La formula evidenzia come si possa migliorare la sicurezza di un sistema in vari modi, per esempio aumentando il numero delle misure adottate (agire sulla sommatoria), variando il peso delle misure esistenti (intervenire sulla consistenza) oppure migliorandone la efficacia (operare sulle strutture e sull'organizzazione).

D'altra parte essa evidenzia che misure di notevole rilevanza possono essere vanificate da un'attuazione inefficace e, viceversa, anche provvedimenti semplici ed a basso costo, se realizzati in maniera efficace, possono innalzare il grado di sicurezza operativa.

Analogamente, esistono svariate proposte per esprimere il concetto di *rischio*. Probabilmente quella più completa e sintetica consiste nella formula:

$$R = \frac{\sum_i P_i \times M_i}{\sum_j K_j}$$

in cui

- P_i è la probabilità (= frequenza) dell'evento i -esimo,
- M_i la sua magnitudo (= conseguenze) e
- K_j sono fattori integrati che tengono conto della informazione e formazione degli esseri umani coinvolti (lavoratori, dirigenti, rappresentanti sindacali, studenti, collaboratori domestici, casalinghe, cittadini, viaggiatori, ecc.), delle protezioni, delle procedure di emergenza, di pronto intervento e così via.

Questa formula dimostra che il rischio collegato ad un evento può essere diminuito agendo sulla probabilità che esso avvenga (intervenendo prevalentemente attraverso la tecnologia), oppure sulle sue conseguenze (soprattutto migliorando l'organizzazione), o sul fattore umano (curando la formazione e l'informazione degli interessati e la loro integrazione con gli aspetti tecnologici ed organizzativi).

ganizzativi).

2. LA SICUREZZA AZIENDALE

La sicurezza di qualunque azienda è affidata ad un complesso sistema costituito da tre parti fondamentali: Tecnologia, Organizzazione ed Uomini.

Nella realtà operativa, per attuare un'efficace e continua protezione, non è sufficiente che le tre componenti vengano progettate, realizzate e rese disponibili, ma risulta assolutamente indispensabile che esse siano anche mantenute efficienti, aggiornate quantitativamente e qualitativamente in base al progresso tecnologico ed alle necessità organizzative, adattate alle mutevoli caratteristiche della società e, attraverso opportune attività di coordinamento e controllo, fatte agire in maniera sinergica.

Questo processo deve svolgersi con continuità nel tempo e nell'intero corpo aziendale.

Ogni sua imperfezione, infatti, si traduce in un mancato, parziale o addirittura controproducente impiego di risorse. Anch'esso pertanto, in relazione alle dimensioni aziendali e quindi alla complessità delle strutture fisiche ed organizzative, assume un costo che può essere notevole e va attentamente valutato e monitorato con gli strumenti di cost benefit analysis, come avviene (o dovrebbe avvenire) per tutti gli investimenti.

L'argomento sicurezza va affrontato anche alla luce delle novità legislative recentemente introdotte nel campo dell'igiene e sicurezza sul lavoro (D. Lgs 626/94 ecc.) e sulla riservatezza delle informazioni (Legge 675/96), che hanno fatto emergere, rafforzandoli notevolmente, i legami e le reciproche influenze esistenti fra i vari aspetti della sicurezza aziendale (security, computer crime, safety e privacy).

3. IL RISCHIO RAPINA NELLE BANCHE ITALIANE

Negli Istituti di Credito il rischio furto - rapina, l'utilizzo e la manutenzione d'impianti, apparecchiature e terminali, gli ambienti e le procedure di lavoro devono essere trattati nell'ambito del nuovo contesto in cui oggi è opportuno operare, secondo un punto di vista molto più complesso rispetto a quello con il quale la gran parte delle aziende affrontava queste problematiche fino a tutti gli anni ottanta. Da qui la necessità di adottare sofisticati strumenti di analisi e controllo di costi e prestazioni, ma anche la creazione di nuove opportunità di sinergia ed ottimizzazione delle risorse tecniche, organizzative ed umane.

E' nota la rilevanza che la sicurezza anticrimine assume in tutti i paesi del mondo e quella antirapina riveste in Italia.

Basti qui ricordare i dati essenziali resi noti dall'ABI con l'ultimo rapporto OSSIF, relativi quindi al 1996, paragonati con la media europea:

	Europa	Italia
Incremento num. rapine rispetto anno preced.	+ 7%	+ 16%
Bottino annuo	195 M\$	75 M\$ (38,4%)
Numero rapine/sportello	1/25	1/11
Probabilità di compimento	n.d.	93%
Autori individuati	n.d.	24%

E' facile rilevare che nel nostro Paese il fenomeno è ancora in crescita e costituisce da solo po-

co meno del 40% dell'intera problematica europea in termini di danno economico, con un numero di rapine per sportello più che doppio rispetto alla media continentale.

Queste considerazioni, insieme all'elevata probabilità di riuscita, al troppo basso rischio di individuazione ed a quello ovviamente ancora inferiore di conseguenze penali, fanno emergere l'importanza economica e sociale del Settore della sicurezza di cui ci interessiamo in queste sedi, cioè il rischio criminoso nelle Banche, con particolare riferimento per quello antirapina del quale approfondiamo alcuni aspetti.

In questa ottica assumono particolare utilità, al fine di valutare ed ottimizzare le prestazioni del sistema di sicurezza ed ottenere la collaborazione di tutti gli organi aziendali, i controlli interni e la documentazione operativa, indispensabile supporto anche per la progettazione di varianti ed implementazioni degli impianti e delle procedure.

Dando quindi per scontata la conoscenza degli aspetti tecnologici ed impiantistici della sicurezza, esaminiamo in maniera schematica due esempi di normativa aziendale, attraverso i quali sarà evidente l'interazione fra le varie componenti della sicurezza (dalla security fino alla privacy, dagli aspetti tecnologici a quelli organizzativi, coordinati e gestiti dall'intervento umano) ed i vantaggi della loro integrazione.

**ESEMPIO N. 1:*****Normativa per l'utilizzo degli accessi dotati di metal detector.***

Fondamentalmente questo tipo di documentazione aziendale deve riguardare almeno i seguenti argomenti:

1. Gestione delle cassettiere;
2. Utilizzo della console operativa;
3. Ingresso clienti riconosciuti e dipendenti di ditte esterne;
4. Ingresso appartenenti alle Forze dell'Ordine;
5. Manutenzione;
6. Procedure di evacuazione.

La redazione della normativa è strettamente collegata dalla realtà fisica dell'agenzia ed alle ulteriori difese di cui essa è dotata; è utile in questa sede sottolineare i seguenti aspetti particolari relativi ad alcuni degli argomenti.

Gestione Cassettiere

- le bussole più moderne sono dotate di sistemi che generano codici randomici e consegnano uno scontrino al Cliente, sul quale è riportato un numero (solitamente di 3 o 4 cifre); con esso è possibile - attraverso la tastiera dedicata - comandare la riapertura dello sportello. Il sistema è ovviamente più costoso, all'acquisto, rispetto a quello tradizionale che prevede l'uso delle classiche chiavette, ma elimina i problemi (ed i costi ...) collegati alla gestione di queste e dei loro duplicati, le lamentele della clientela per la perdita di oggetti, i rischi connessi all'utilizzo da parte di terzi delle cassette per lo scambio illegale di beni (tipicamente droga) con coinvolgimento della Banca, ecc.

Ingresso delle Forze dell'Ordine

- In situazione non di emergenza, l'ingresso di persone armate che si dichiarano appartenenti alle FF. OO. deve essere preceduto dall'esibizione del tesserino e da telefonate al Comando di appartenenza, previo controllo del numero sull'elenco telefonico (ovviamente la stessa procedura vale per l'arrivo inatteso di dipendenti di Istituti di Vigilanza).

Procedure di evacuazione

- Il comportamento dell'addetto alla console di gestione della bussola deve essere concordato con il Responsabile del Servizio di Prevenzione e Protezione e conforme al piano di evacuazione dell'agenzia.

ESEMPIO N. 2:***Verbale di constatazione dell'Ispettorato Interno***

L'ispettorato Interno, nell'ambito della funzione che normalmente svolge o in occasione di verifiche mirate, deve controllare anche lo stato delle misure di sicurezza.

Le operazioni, ed il relativo verbale, devono riguardare almeno i seguenti punti:

1. Accesso negli stabilimenti;
2. Utilizzo degli accessi dotati di metal - detector;
3. Uscite di emergenza;
4. Impianti antifurto, anticendio e Tvcc;
5. Mezzi forti;
6. Combinazioni e chiavi dei mezzi forti;
7. Altri mezzi antirapina;
8. Vigilanza armata;
9. Cassette e Pacchetti di medicazione;
10. Estintori;
11. Libro Matricola, Libro Infortuni e documentazione tecnico/amministrativa.

Si consiglia di redigere uno schema di verbale di constatazione da divulgare nell'ambito della Banca. Basandosi su esso, ogni Preposto potrà, almeno una volta all'anno, effettuare una autoverifica dello stato della sicurezza presso la propria agenzia e provvedere per eliminare eventuali carenze o segnalarle agli organi competenti, realizzando un rapido ed efficace sistema di controllo diretto, omogeneo in tutta l'azienda.

CONCLUSIONI

Riflettendo sugli esempi sinteticamente esposti o, meglio ancora, provando a metterli in pratica come avremmo potuto fare in questa sede se avessimo avuto sufficiente tempo a disposizione, si evidenzierà la strettissima interconnessione che ormai esiste tra security, safety e gli altri aspetti della sicurezza, con le opportunità che ciò comporta per la realizzazione di sinergie.

Altrettanto chiara risulterà l'importanza che assume, in termini sia di efficienza che di efficacia, una stretta integrazione fra le componenti tecnologiche, organizzative ed umane del sistema di sicurezza aziendale. La loro correlazione, attraverso una struttura organizzativa costituita da procedure certe ed omogenee, innalzerà sicuramente l'entità e la qualità del risultato finale conseguibile con gli investimenti effettuati e consentirà una loro gestione più consapevole da parte dei vertici aziendali.

Questi due concetti devono essere i principi ispiratori di tutto l'operato del Responsabile della Sicurezza aziendale, particolarmente per quanto attiene la valutazione del rischio criminoso e l'impostazione dei rapporti con gli altri organi della Banca.