

UNA NUOVA METODOLOGIA PER LA VALUTAZIONE DELLE DIFESE E DEI RISCHI PER LA DETERMINAZIONE DEL LIVELLO DI SICUREZZA DEI SITI BANCARI

P.I. MICHELE MESSINA

Dirigente dell'Ufficio Prevenzione dell'A.N.I.A.

Ciascun Istituto di credito ha, in generale, al suo interno le competenze per poter scegliere le misure di sicurezza da adottare al fine di prevenire il verificarsi di eventi criminosi e di tutelare la sicurezza dei dipendenti e della clientela. Ma, mentre le banche dei grandi centri urbani sono, di regola, provviste di sofisticati sistemi di sicurezza, spesso, quelle dei piccoli paesi, ovviamente in proporzione al grado di criminalità in essi presente, sono munite di un livello minimo o addirittura insufficiente di misure di prevenzione. Tale situazione, ha spinto la criminalità organizzata a prendere di mira qualsiasi dipendenza bancaria, senza distinzione ed ovunque essa sia collocata.

LE METODOLOGIE DI ATTACCO

La rapina rappresenta ancora il reato più frequentemente commesso a danno delle banche, tuttavia, sono radicalmente mutate in questi ultimi anni le metodiche di esecuzione. Molte rapine, infatti, vengono commesse con tecniche fino a pochi anni fa impensabili; in parecchi casi le vittime vengono ipnotizzate o narcotizzate all'interno dello sportello, oppure ancora vengono presi e tenuti in ostaggio i familiari fino a che l'evento non sia stato portato a termine con successo dai criminali; vengono utilizzate armi improprie quali: siringhe infette, coltellini multiuso, punteruoli di plastica ecc. Questi strumenti, per altro, possono essere portati all'interno dell'agenzia bancaria senza essere rilevati dai *metal detector*, apparecchiature che erano state create, appositamente, per segnalare la presenza di armi da fuoco e di altri oggetti metallici di possibile offesa, più tipicamente utilizzati dai rapinatori professionisti.

Riguardo ai furti, l'obiettivo principale dell'attacco dei criminali è il "bancomat" allo scopo di asportarne il denaro in esso contenuto. L'apertura dei battenti del contenitore avviene, normalmente, per esplosione, dopo aver introdotto al suo interno una miscela di gas detonante. I danni ai locali della banca, derivanti da questi attacchi, possono essere anche ingenti e non è possibile escludere che vi sia un coinvolgimento di vite umane.

Altro motivo di preoccupazione è rappresentato dalla cosiddetta "*criminalità dei colletti bianchi*", cioè i danni da "infedeltà" commessa dai dipendenti. Questo fenomeno, negli ultimi anni, ha raggiunto dimensioni insopportabili e che potrebbero determinare la chiusura dei mercati riassicurativi per i rischi italiani.

Non si può più sottovalutare, inoltre, il fenomeno del terrorismo; i tragici fatti di cronaca di questi giorni che hanno colpito, in sequenza, gli Stati Uniti, la Francia ed altri Paesi del mondo ne sono un esempio fin troppo eloquente. I gruppi terroristici hanno bisogno di impossessarsi di grandi quantità di denaro per organizzare le loro micidiali azioni, pertanto le cellule di questi gruppi, allo scopo di finanziarsi, non esitano a commettere ogni tipo di crimine. A differenza del rapinatore, che cerca di fare di tutto per evitare che ci scappi il morto, il terrorista, in conformità alla sua ideologia ed ai suoi obiettivi politici, tende ad uccidere chiunque tenti di ostacolarlo nel compiere la sua azione criminosa anche allo scopo di consentire la maggiore risonanza possibile all'evento. Pensiamo solo per un istante cosa potrebbe accadere se un "*kamikaze*", imbottito di esplosivo, che volesse colpire gli interessi di un determinato gruppo multinazionale, si facesse esplodere all'interno di un'agenzia

bancaria appartenente a quel gruppo o che avesse lo stesso come cliente primario. Il danno sarebbe incalcolabile, soprattutto in termini di vite umane e di immagine. Non possiamo dimenticare, a tal proposito, quanto accadde, nel lontano dicembre del 1969, all'interno dell'agenzia di una banca nazionale, ubicata in piazza Fontana, a Milano. L'attentato in quell'occasione causò numerose vittime e ingenti danni. Ma anche l'attacco terroristico dell'11 settembre scorso, a New York, ha avuto come conseguenza la sparizione, in quell'enorme massacro, di una delle sedi più prestigiose della *Chase Manhattan Bank*, che aveva sede all'interno delle due Torri gemelle.

COME PREVENIRE I NUOVI CRIMINI

Da quanto sopra, deriva che vi è la necessità di riconsiderare totalmente i concetti di sicurezza bancaria fin qui applicati per prevenire le azioni criminose. Devono essere ora analizzati, in maniera più approfondita, i sinistri verificatisi al fine di valutare meglio quale sia stato il grado di vulnerabilità delle difese presenti, nel corso di tali eventi. La sicurezza anticrimine non può più essere vista in maniera disgiunta da quella antinfortunistica; la sicurezza sul lavoro è un tema prioritario che deve essere affrontato ogni qualvolta si analizzano i rischi aziendali. Questo approccio è stato, più volte, sancito anche dalle numerose leggi europee e nazionali vigenti in materia (DPR 547/55, DPR 303/56, D.Lgs. 626/94, ecc.).

Già l'articolo 2087 del Codice Civile ha stabilito che il datore di lavoro è tenuto a garantire la massima sicurezza in funzione di quelle che sono l'esperienza, la tecnologia del momento e la particolarità del lavoro; egli è tenuto quindi a porre in essere tutte le misure necessarie per evitare il verificarsi di danni alla salute e alla integrità fisica del lavoratore. A questo proposito, è opportuno citare la sentenza del 6 settembre 1988, n. 5048, della Suprema Corte che ha condannato un Istituto di credito al risarcimento dei danni nei confronti di un dipendente rimasto ferito durante una rapina verificatasi in una sede la cui porta di ingresso era munita di un congegno automatico di apertura risultato difettoso. Le nuovissime tecnologie di controllo degli accessi presenti nel mercato, ad esempio, ci aiutano a prevenire i rischi poiché consentono di filtrare l'accesso delle persone in banca - anche per mezzo di particolari tecniche biometriche - mantenendo inalterate la *safety* e l'operatività dell'agenzia.

Nel corso della precedente legislatura, sono stati presentati alcuni disegni di legge, da parte di parlamentari di vari gruppi politici che, in sostanza, prevedevano che fosse demandato al Ministero dell'Interno il compito di stabilire, per decreto, i criteri ed i requisiti di prevenzione e protezione anticrimine da attuare, obbligatoriamente, in prestabiliti settori di attività, tra i quali erano state incluse anche le banche. E' opportuno rammentare che lo stesso Ministero svolge da molti anni attività normativa nel campo della prevenzione incendi. Altri simili precedenti li troviamo in alcuni Paesi europei quali, ad esempio, la Spagna, la Francia, il Belgio e l'Olanda, ove esistono apposite normative di legge che impongono a molti settori di attività, tra cui le banche, l'adozione di idonee misure di sicurezza mirate, essenzialmente, a prevenire i rischi di furto e di rapina.

E' fondamentale quindi cercare di rendere omogenea una materia così delicata qual'è la sicurezza anticrimine che finora è stata lasciata, un pò, alla libera interpretazione di tutti gli operatori del mercato. Ci dobbiamo, inoltre, rendere conto, realisticamente, che le misure di prevenzione esistenti all'interno di determinate attività ed in particolare degli istituti di credito, in parecchi casi, non sono più sufficienti a fronteggiare i mutati rischi del nuovo millennio.

Il grado di appetibilità di un sito bancario per le organizzazioni criminali e terroristiche operanti nel nostro Paese, anche a causa dell'imminente passaggio dalla lira all'euro, sarà, nel prossimo futuro, assai più elevato e, conseguentemente, ci dobbiamo aspettare una forte *escalation* di attacchi a danno di questo vitale settore di attività.

La maggior giacenza di denaro all'interno delle agenzie bancarie, durante tutto il periodo del *changeover*, impone quindi, fin d'ora, agli Istituti di credito la risoluzione di problematiche di sicurezza certamente difficili e complesse. Si dovrà prevedere, in ogni caso, un sensibile aumento delle rapine, delle estorsioni, delle truffe e dei furti. A conferma di quanto asserito, è opportuno ricordare che il nostro Paese è stato il primo dell'U.E. a subire, nello scorso mese di settembre, una rapina di monete euro, per altro, non ancora entrate ufficialmente in circolazione.

Occorre poi considerare che ogni dipendenza bancaria e diversa dalle altre per ubicazione, caratteristiche costruttive, numero di dipendenti, quantità di valori in essa giacenti, ecc. Tali fattori, la cui elencazione non vuole essere esaustiva, debbono essere attentamente valutati in fase di analisi del rischio al fine di potere predisporre un progetto di sicurezza congruo con le reali esigenze di protezione di ciascun sito.

L'ANALISI DEL RISCHIO

Per analisi di rischio si intende, più comunemente, quel complesso di valutazioni e studi orientati essenzialmente alla determinazione delle probabilità di accadimento di un evento dannoso, tendenti anche a stabilirne la sua ampiezza (magnitudo), nell'ottica di tenere sotto controllo e "dominare" il rischio. L'analisi dovrà tenere altresì conto delle dinamiche dei sinistri accaduti in precedenza e della statistica. Maggiore è la quantità di informazioni e di dati che possano essere soggetti ad analisi e che riguardino una determinata tipologia di rischio, tanto più elevata sarà la qualità dei risultati dell'analisi stessa e quindi la conoscenza del rischio. Allo scopo di definire i necessari interventi di prevenzione occorre, innanzi tutto, precisare gli obiettivi, delimitare le aree di interesse, formulare le opportune strategie, adottare specifiche metodologie di analisi delle singole problematiche, infine, tradurre in pratica le azioni.

Come per lo studio della prevenzione degli eventi accidentali (alluvioni, terremoti, incendi, inondazioni), anche nel caso degli eventi dolosi, connessi con il crimine (furti, rapine, estorsioni, attentati ecc.) è possibile applicare il metodo della "*valutazione probabilistica del rischio*" che, nella fattispecie, dovrà tenere conto, tra l'altro, anche di elementi quali: il grado di appetibilità del bene patrimoniale che si vuol proteggere, il modo di custodia, il suo valore intrinseco, la sua collocazione nel territorio ecc.

Il furto rappresenta, all'incirca, il 90% dei reati contro il patrimonio e troppo spesso viene, da molti, considerato alla stregua di un moderno flagello biblico contro il quale non è possibile difendersi. E' sconcertante dover sottolineare che in Italia, ancora oggi, nel 95% dei casi di furto gli autori rimangono ignoti, mentre tale percentuale si dimezza nei casi di rapina.

LA SICUREZZA INTEGRATA

Il nuovo approccio adottato dai professionisti della sicurezza più preparati nella progettazione dei sistemi di prevenzione e protezione si basa ormai sull'integrazione delle diverse tecnologie applicabili. Sono essenzialmente tre i fattori importanti che caratterizzano un sistema di sicurezza integrato:

- l'affidabilità, cioè la garanzia che il sistema considerato assolva alle sue funzioni nelle condizioni prestabilite, senza interventi straordinari di riparazione, oltre quelli minimi previsti di manutenzione ordinaria;
- la disponibilità, definibile come l'intervallo di tempo in cui il sistema risulta correttamente funzionante ed efficiente;

- la probabilità di intervento del sistema, cioè la sua risposta alla sollecitazione derivante dalla rilevazione di un determinato evento.

Il sistema di sicurezza deve prevedere, inoltre, un sufficiente grado di ridondanza e di diversificazione dei suoi componenti più importanti; ciò consentirà di ridurre in maniera significativa la frequenza di accadimento di anomalie e guasti, aumentando, nel contempo, il suo grado di affidabilità. Tali importanti caratteristiche potrebbero portare ad una sensibile lievitazione dei costi della sicurezza ed allora si renderà necessario riequilibrare, opportunamente, nella fase di progettazione, le misure di prevenzione che dovranno risultare commisurate alle reali esigenze di protezione del sito. Dovrà essere attuato, in ogni caso, un livello minimo di sicurezza al di sotto del quale non si potrà scendere, pena l'annullamento degli effetti della prevenzione.

Un buon sistema integrato di prevenzione è assimilabile ad una catena la cui robustezza è commisurata a quella del suo anello più debole. Pertanto, nell'accingersi a progettargli, ogni sua singola componente dovrà essere opportunamente calibrata, in maniera che possa opporre un'adeguata resistenza, secondo il suo grado di esposizione e nell'ottica di conferire al sistema stesso un grado di sicurezza, complessivamente, uniforme.

Il sistema in questione è costituito, di regola, da tre fondamentali componenti:

- le misure di difesa passive (meccaniche);
- le misure di difesa attive (elettroniche);
- la gestione umana.

Qualsiasi considerazione sulle misure di prevenzione e protezione dei rischi deve partire dal presupposto che in "assoluto" non esistono difese invulnerabili. Il grado di resistenza offerto da una difesa è strettamente correlato al tempo che il ladro impiega a superarla, in base alla sua esperienza ed agli strumenti in suo possesso. Per queste ragioni, alla prevenzione è indispensabile affiancare anche la polizza di assicurazione.

L'ATTEGGIAMENTO DEGLI ASSICURATORI

Alla luce delle mutate situazioni di mercato e del conseguente sensibile aumento dell'ampiezza dei danni (le rapine infatti hanno subito una lieve flessione in termini di frequenza ma è aumentata, fortemente, l'entità di danno medio), gli assicuratori ritengono che sia giunto il momento di rivedere le loro politiche commerciali e di rivalutare maggiormente il ruolo della prevenzione, in particolar modo, in un settore ad altissimo rischio qual'è quello bancario.

A tale scopo, sarebbe auspicabile creare un gruppo di studio costituito da tecnici esperti del settore della sicurezza dei comparti bancario e assicurativo cui affidare il compito di affrontare l'intera problematica, non trascurando il fenomeno dell'"*infedeltà*", le sue cause interne ed esterne, e verificare, nel contempo, la validità dei vigenti regolamenti inerenti i servizi di audit interno bancario. Infine, giungere a definire, in tempi brevi, uno strumento di valutazione dei rischi riferibili alle agenzie bancarie che possa permettere di adottare, in base alla classe di rischio identificata, le necessarie misure, opportunamente integrate, di prevenzione e protezione.

Tale azione comune, per altro, già collaudata con discreto successo in passato, potrebbe permettere anche la creazione di schemi, che in parte sono già utilizzati dagli operatori dei due settori, che dovrebbero essere aggiornati dal punto di vista non solo tecnico ma anche socio-politico ed essere adeguatamente armonizzati.