

Come difendere l'impresa dal pericolo delle frodi

Alberto Nobili, CPP

CSO di ATF Bank (Kazakistan), Socio AIPSA e ASIS

Le strategie da attuare per fronteggiare un fenomeno che comporta danni patrimoniali pari ogni anno al 2,1% del fatturato. Le figure professionali da utilizzare

In un recente report pubblicato da un'azienda internazionale leader nel campo delle investigazioni e consulenze, è stato evidenziato come, nel solo anno 2011, il danno patrimoniale derivante da **fenomeni fraudolenti** abbia inciso in media sul 2,1% dei ricavi delle aziende a livello mondiale. Come spesso evidenziato da analoghi report e ricerche su questo tema, gran parte degli illeciti, circa il 60%, sono per altro commessi da dipendenti interni alle aziende stesse e la percentuale appare invariata se non in aumento negli ultimi anni.

Per sgombrare il campo da equivoci è doveroso però precisare che in ambito internazionale, e più in particolare nel mondo anglosassone, il termine "*fraud*", frode nel contesto di questo articolo, non si limita ad indicare la sola fattispecie di truffa così come descritta dal nostro Codice Penale, ma il concetto si estende invece a molteplici condotte intenzionali che possono, a se-



conda dei casi, configurare violazioni di norme e regolamenti.

Queste considerazioni, che non sono nuove e non sorprendono chi opera abitualmente nel campo della security, servono da *incipit* ad una premessa essenziale. Il primo passo verso un **approccio effettivo alla prevenzione delle frodi** è dato dalla volontà del management di creare un ambiente di lavoro quanto più possibile integro e trasparente. Un ambiente di lavoro in cui la cultura dell'onestà e la condivisione dei valori etici siano costantemente promosse ed ispiratrici del comportamento leale e corretto di ogni singolo dipendente.

La stretta osservanza di **procedure e regolamenti interni**, il senso di appartenenza nonché la consapevolezza del rischio derivante da negligenza e superficialità nelle attività quotidiane, rappresenterebbero

già di per sé un ostacolo concreto alla commissione di frodi ed illeciti ai danni dell'azienda.

Nonostante ciò è bene però ricordare che nella vita di un'azienda, a prescindere dal settore in cui essa opera, la tematica delle frodi, dalla loro definizione, alla **prevenzione e gestione**, rappresenta uno dei problemi operativi di più difficile risoluzione. In questo campo non esistono ancora soluzioni tecnologiche omnicomprehensive, prodotti miracolosi, o ricette magiche che da sole possano risolvere un tale problema.

La molteplicità dei modi in cui ciò che definiamo frode può realizzarsi, in mancanza di processi o pratiche consolidate, può però far sì che spesso diverse funzioni si sentano allo stesso tempo investite della responsabilità di gestire coordinare ed interloquire con il vertice aziendale su que-



Alberto Nobili

sto tema specifico. Così accadendo succede che il management abbia spesso una **percezione non chiara** del fenomeno poiché gestito ed analizzato da diversi soggetti che, in base alla propria visione ed al ruolo che all'interno dell'azienda ricoprono, danno un'lettura non sempre uniforme ed obbiettiva sulla problematica.

E ciò spesso avviene poiché l'approccio alle frodi quasi sempre finisce con l'essere reattivo piuttosto che preventivo, settoriale piuttosto che globale.

Dando per assodato che nell'attività di contrasto alle frodi si possano distinguere lo-

“*La tematica delle frodi, dalla loro definizione, alla prevenzione e gestione, rappresenta uno dei problemi operativi di più difficile risoluzione*”

gicamente e cronologicamente **due fasi** ben distinte e cioè **prevenzione e reazione**, questo articolo si propone di illustrare un possibile approccio metodologico alla prevenzione delle frodi senza però soffermarsi sul tema della reazione e gestione delle stesse.

Ecco allora che se un'azienda si proponesse per la prima volta di voler affrontare il problema della prevenzione delle frodi dovrebbe prima di tutto iniziare con il **concordare** al suo interno una definizione condivisa di frode e cioè rispondere alla domanda: che cosa si intende per frode all'interno dell'azienda?

La mancanza di tale definizione potrebbe creare confusione, generare fraintendimenti ed allargare a dismisura il perimetro dell'attività.

La scelta adottata da molte aziende è quella di creare funzioni di **Fraud Preven-**

tion con un focus limitato a determinati processi di business come spesso accade per esempio nel settore finanziario, assicurativo o delle telecomunicazioni. In questi settori si riconosce infatti alla funzione di Fraud Prevention il compito di contrastare e prevenire tipologie di minacce ben definite, statisticamente ricorrenti e nella maggior parte dei casi provenienti dall'esterno. E' il caso ad esempio delle strutture di Fraud Prevention che operano nel campo della **monetica** o dei servizi di online banking. In questi casi parliamo di strutture di prevenzione operativa vera e propria che utilizzano metodologie supportate da applicazioni informatiche anche di tipo “**a regole**” o “**neurali**”.

Questo approccio è certamente il più diffuso, efficace ed efficiente qualora in ambito aziendale, a prescindere dalle definizioni tecnico-giuridiche, si sia deciso di far coincidere con il termine frode un insieme di minacce ben identificate e tipicizzate. Se invece la decisione presa è stata quella di adottare una definizione più generica di frode e definirla cioè come ogni **comportamento intenzionale**, attivo od omissivo, che consenta l'acquisizione di un vantaggio personale o terzo e che possa causare un danno diretto od indiretto ad un'azienda, ecco che allora la prevenzione delle tipologie residuali di minacce dovrà essere invece affidata e trattata da diverse funzioni aziendali quali l'HR, l'Audit, l'Operational Risk Management od il Legale.

Adottando un'accezione così ampia del termine appare chiaro come un'unica funzione non sarebbe da sola in grado di affrontare le molteplici manifestazioni del fenomeno frode, che necessiterà invece di un approccio comune, multifunzionale e trasversale.

In questo caso, ciò che però risulterà fondamentale è l'assicurarsi che la strategia ed il coordinamento delle varie iniziative, che andranno a costituire l'ossatura della capacità di prevenzione delle frodi, siano

affidati ad un' **unica figura** che potrà essere sia un manager interno che un consulente esterno in base alle esigenze ed alle scelte dell'azienda.

A questa figura dovrà essere affidata la responsabilità di svolgere un **risk assessment** iniziale che individui all'interno di ogni area dell'azienda la tipologia di frode realizzabile, il relativo *modus operandi*, i potenziali autori, il tipo e l'intensità del danno sia diretto che indiretto, nonché la probabilità di accadimento.

Il risultato del risk assessment, che dovrà ciclicamente essere rivisto ed aggiornato ed accompagnato da un'attività di costante ricerca e studio del fenomeno, sarà lo strumento su cui basare la futura strategia di prevenzione attraverso l'introduzione di misure organizzative, procedurali e/o tecnologiche.

Tra le varie e possibili misure organizzative potrà esservi la **revisione del codice etico**, la stesura di nuove politiche, l'attribuzione o redistribuzione della responsabilità in capo alle varie funzioni aziendali in tema di prevenzione e gestione delle frodi, la revisione dei meccanismi di coordinamento, la definizione di programmi di **training and awareness** e persino la decisione di creare *ex novo* una funzione di Fraud Prevention dedicata al contrasto di quegli eventi a maggiore incidenza sul patrimonio aziendale. Le misure di prevenzione procedurali consisteranno soprattutto nella revisione dei processi interni e di business maggiormente a rischio e l'inserimento di elementi di controllo basati su concetti semplici quanto fondamentali ed internazionalmente riconosciuti quali: *four eyes principle*, *segregation of duty*, *need to know basis*.

Le **misure tecnologiche** troveranno invece applicazione in funzione preventiva laddove permetteranno di ridurre significativamente il margine di errore ed interazione umana all'interno dei processi aziendali, garantiranno un maggior rispetto ed aderenza alle politiche di sicurezza delle infor-

mazioni, forniranno un ausilio nell'analizzare volumi significativi di dati che altrimenti passerebbero inosservati. L'ausilio fondamentale dei software di prevenzione delle frodi risiede infatti nella loro grande capacità di analisi e tracciabilità delle operazioni che permette di riconoscere tempestivamente fattori di rischio e portare all'attenzione degli operatori degli alert che verranno successivamente investigati dalla funzione preposta. Così come i risultati delle investigazioni anche le lezioni acquisite (*lessons learnt*) dovranno essere raccolte e documentate al fine di non disperdere questo prezioso patrimonio informativo che se ben gestito all'interno di database dedicati, potrebbe facilitare la prevenzione di eventi futuri.

La prevenzione delle frodi così intesa dovrà pertanto essere fortemente supportata ed interiorizzata dal vertice aziendale fino a divenire parte integrante della cultura aziendale stessa. Non è con l'adozione di strumenti singoli o attività a sé stanti che la problematica possa essere affrontata.

La responsabilità per tale attività non dovrà essere pertanto attribuita ad un'unica funzione poiché il suo successo sarà garantito dallo sforzo congiunto di più funzioni i cui progetti e le cui iniziative siano abilmente coordinati, in maniera univoca, verso il raggiungimento di un comune obiettivo.

Questa breve esposizione ha voluto quindi descrivere e toccare i temi principali necessari allo sviluppo di una moderna strategia di prevenzione delle frodi.

Tuttavia va da sé che la complessità sottostante ognuno dei passi metodologici sopra descritti meriterebbe un'appropriata analisi ed un adeguato approfondimento. Quanto scritto, che è frutto di esperienze dirette e progettuali in strutture complesse ed internazionali, ci si augura possa fornire uno spunto di riflessione, discussione o rielaborazione critica di quanto fino ad ora fatto in questo ambito.