

**Sicurezza.** Secondo l'agenzia investigativa Kroll le frodi industriali causano una perdita annua di 7 milioni di dollari l'anno

# Spiate quattro aziende su dieci

## Il 65% delle organizzazioni finanziarie italiane subisce violazioni della security

**Rita Fatiguso**  
MILANO  
Quattro aziende su dieci nel mondo sono vittime di frodi industriali, specie furti di know how, con una perdita media annua di 6 milioni e 700mila dollari. «L'Italia, con la sua rete di piccole e medie imprese iperspecializzate ha il primato della vulnerabilità» - precisa da Londra Matteo Bigazzi, della detection prevention investigation unity dell'agenzia di security Kroll - da cinque anni la tensione resta alta. Al di là delle cifre il furto di un modello industriale "girato" a società concorrenti all'estero diventa una sentenza di morte».

**I dati chiave.**  
Secondo il Kroll Global Fraud Report 2007 dell' Economist Intelligence Unit realizzato su un campione di 900 top manager, un'azienda su dieci accusa perdite per frodi oltre i 100 milioni all'anno, quasi la metà si sente più esposta di tre anni fa.

«I furti di Intellectual property sono all'ordine del giorno, ma l'Italia è davanti alla Germania, a Singapore, all'India - aggiunge Bigazzi - Il settore finanziario ha più dell'80% delle sedi vittime della violazione delle regole di governance, delle frodi finanziarie interne, degli attacchi informatici. Il 47% delle industrie manifatturiere ha subito furti, il 23% attentati alla proprietà intellettuale».

La disputa Ferrari-McLaren, con la connessa feroce guerra di email pirata, testimoniano uno scenario incandescente. Salute, farmaceutica e biotecnologie hanno contabilizzato danni anche del 75% superiori al triennio

precedente. Il 28% delle aziende del settore hi-tech, media e telecomunicazioni ha subito furti.

Spariscono da computer e cassette mailing list, monitoraggi della clientela, studi di fattibilità, disegni industriali tenuti sotto chiave ma non brevettati. E spesso spariscono con il passaggio ad altra azienda di dipendenti, manager o consulenti.

Esemplare il caso pendente davanti ad un tribunale del Nord Italia, una storia nata l'anno scorso quando un'importante azienda meccanica leader nel proprio settore, ha

### MAGLIA NERA

Il nostro Paese precede Germania, Singapore e India per il numero di reati in materia di proprietà intellettuale

### PIÙ FONDI IN CAMPO

Il 98% delle banche intervistate da Deloitte ha aumentato il budget per difendersi dalle incursioni informatiche

citato in giudizio una diretta concorrente, rea di aver sottratto segreti industriali di importanza strategica. Dal 2001 la seconda azienda aveva iniziato a far collaborare l'ex direttore generale della prima, i cui clienti ben presto sono stati

contattati con offerte di integrativi di fornitura. Nomi conservati in una banca dati di proprietà della società che conteneva anche informazioni tecniche utili per progettare sofisticati e costosi macchinari. Ebbene, la seconda socie-

tà è riuscita a lanciare sul mercato macchinari con le caratteristiche presenti nella banca dati, dalla quale era stata saccheggiata non solo la clientela attuale ma anche quella potenziale legata al giro dei pezzi di ricambio.

Appena due anni fa, grazie a un decreto di riforma del Codice di proprietà industriale, anche il know how ha trovato una tutela all'altezza di quella accordata a marchi e brevetti (si veda articolo in basso). Dice Elisabetta Racca, avvocato, esperta del settore: «Le informazioni riservate sono parificate ai diritti di proprietà industriale. Ma la segretezza va protetta con misure idonee interne ed esterne, anche inserendo clausole nei contratti di lavoro o di collaborazione per informarli dell'esistenza di un segreto meritevole di tutela».

«La pletera di dipendenti o, peggio, di collaboratori a contratto, consulenti, precari, lavoratori di passaggio, ai quali poco importa la fedeltà all'azienda, è una grave fonte di rischio - dice Massimino Boccardi, esperto di security di Hewlett Packard, docente di *Indagini su crimini via computer* al master dell'Associazione di giornalismo investigativo - specie nel credito, nelle assicurazioni, nella finanza, settori che, in linea con le regole di Basilea 2, devono rafforzare la sicurezza».

### Il fattore umano.

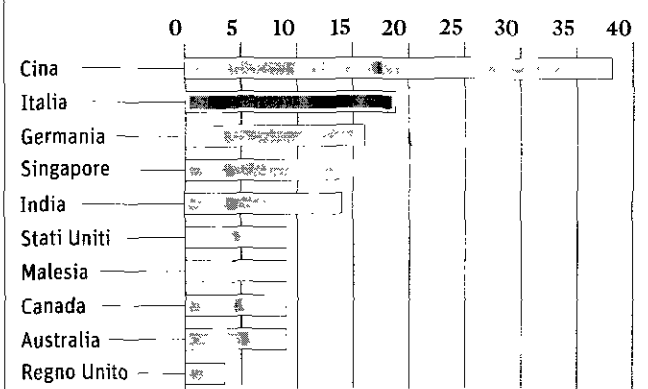
Anche il «Global Financial Services Security Survey» 2007 di Deloitte individua nel fattore umano la prima causa di violazione dei sistemi di sicurezza bancaria: il 65% delle organizzazioni finanziarie in Italia ha subito violazioni dei sistemi di sicurezza dall'ester-



**Licenziato.** L'ingegnere britannico Nigel Stepney è stato al centro della spy story dell'estate tra Ferrari e McLaren. Sospeso dall'incarico dopo essere stato indagato per presunto sabotaggio e spionaggio industriale ai danni della scuderia italiana, è stato infine licenziato dalla Ferrari.

### I FURTI DI PROPRIETÀ INTELLETTUALE

Percentuale di imprese colpite da spionaggio industriale negli ultimi tre anni



Fonte: Kroll Global Fraud Report

### 40%

**Le aziende colpite**  
Quattro aziende su 10 nel mondo sono vittime di frodi industriali

### 6,7

**I danni**  
Si calcola che la perdita media

annua per le aziende sia di 6,7 milioni di dollari

### 47%

**Industria**  
La percentuale di aziende manifatturiere che ha subito furti di proprietà intellettuale in Italia. Salute e biotech tra le più colpite

no, ma quasi un terzo (31%) da dipendenti.

«Le imprese si proteggono dai colpi bassi - aggiunge Massimino Boccardi - con sistemi che permettono di monitorare i comportamenti, videocamere e software che garantiscono la tracciabilità. Ma quando l'anomalia viene intercettata, dobbiamo buttare l'amo. Così abbiamo scoperto un dipendente di una banca che passava al setaccio i conti di una cinquantina di clienti, a scopo di riciclaggio, è stata dura, ma ce l'abbiamo fatta. Lui, ovviamente, ha perso il posto».

«Le prove - aggiunge Umberto Repetto, esperto di criminalità informatica della Guardia di Finanza - sono l'elemento più difficile da ricostruire. Gli attacchi degli hackers richiedono troppi fondi e poi ci vuole sempre una talpa all'interno, che sia la donna delle pulizie o un dipendente infedele, non cambia. Le pen drive, rendono tutto più semplice. Quanto alla clonazione, quella dei siti è superata dalle finte e-mail aziendali per carpire informazioni riservate».

Le banche intervistate da Deloitte (98%) indicano un aumento dei budget per la sicurezza. Il 35% pensa che l'investimento sia inadeguato, mentre il 98% segnala un'impennata dei fondi.

Un consulente marketing di vari gruppi della grande distribuzione, però, è chiaro: «La tecnica più antica, sulla cui efficacia micidiale io potrei davvero giurare e dalla quale bisogna guardarsi è basata sulla memoria visiva. Immagazzinare i dati diffusi in una riunione, beh, contro questo metodo non c'è tecnologia che tenga».

## Dall'Asia il 46% degli attacchi Nord-Est, le Pmi bersaglio di hacker cinesi

**Serena Uccello**  
MILANO

Secondo il Times il Pentagono avrebbe pronto un rapporto: secondo gli esperti Usa, Pechino avrebbe messo a punto un piano di cyber-attacco in grado di annullare le difese americane. Decine di hacker abilissimi sarebbero al servizio dell'esercito cinese. Fantapolica? Forse. Quel che è certo è che questi presunti attacchi potrebbero essere, nonostante le smentite del governo cinese, solo un aspetto o una piccolissima parte di un fenomeno più diffuso e pericoloso che coinvolge anche l'Italia. Dall'inizio del 2007 ad oggi, infatti, l'Osservatorio Nazionale per la Sicurezza Informatica ha rilevato su un campione di 500 pmi ben 122.500 attacchi informatici, il 46% dei quali provenienti proprio dalla Cina.

Tentativi di intrusione principalmente rivolti verso aziende italiane del Nord Est finalizzati non al danneggiamento del sistema informatico aziendale ma alla sottrazione di informazioni riservate. In sintesi: spionaggio aziendale. Si tratta di incursioni ripetute con l'obiettivo di copiare modelli, design, brevetti. Lo dice l'analisi della tipologia di attacco realizzata dalla Yarix, un'azienda che si occupa della sicurezza informativa di diverse imprese, che ne ha anche studiato la provenienza.

Per il 49% sono attacchi collegabili a server cinesi, nel 25% dei casi la provenienza è turca, per il 15% brasiliana. La vulnerabilità maggiore sta nel web: basta infatti avere il sito internet e magari anche un'area del sito riservata ai clienti che il rischio di incursioni diventa altissimo.

La rete può dunque trasformarsi in una porta di accesso alle casseforti di ogni azienda, ovvero al portafoglio clienti e ai fornitori, quando appunto non agli archivi.

E che la soglia del pericolo per queste aziende sia cresciuta è confermato anche dalla Poltel di Treviso che se fino a quattro anni fa contava tre o quattro di queste azioni, oggi ne registra una ventina: «Spesso si tratta di sottrazione di dati finalizzati alla concorrenza sleale, qualche volta anche con la complicità di dipendenti infedeli», spiega

### BENI DA TRAFUGARE

Nel 2007 registrati 122mila episodi su un campione di 500 imprese: nel mirino soprattutto design e brevetti

un investigatore.

La casistica è vasta. «Un esempio da manuale - spiega Mirko Gatto, presidente di Yarix - è quello che ha coinvolto di recente un nostro cliente. L'addetto commerciale dell'azienda aveva trascorso un mese in Cina, al suo ritorno in ufficio, in Italia, subito dopo l'accensione del suo portatile dal nostro centro informatico abbiamo notato la presenza di attività anomala. Ci siamo così messi in contatto con il cliente - racconta ancora Gatto - perché dai nostri monitor avevamo cominciato a registrare diversi tentativi di connessione non autorizzati da una località remota della Cina».

La reazione tecnica è immediata. L'attacco, questa volta, viene bloccato.

Poche certezze dalla giurisprudenza in materia di informazioni riservate

## Il segreto? È un «fatto relativo»

**Beatrice Dalia**  
MILANO

Segreti e misteri. La giurisprudenza sulle invenzioni industriali ha più punti interrogativi che risposte. Quali informazioni interne ed esterne al processo produttivo sono riservate e quanto lo sono è tutto da dimostrare. Le poche sentenze di cui si ha conoscenza, però, consentono un riepilogo dei punti fermi all'indomani del Dlgs 30/2005 sul tema.

### Quali segreti

Intanto, «non sussiste sottrazione di informazioni riservate in assenza di prova che le informazioni sottratte siano segrete». Con questa affermazione il Tribunale di Venezia (ordinanza dell'8 marzo 2006) ha messo subito in chiaro gli oneri a carico dei "proprietari" delle conoscenze.

Prima di poter gridare al ladro devono dimostrare ai giudici di aver utilizzato tutte le password e i lucchetti del caso.

A sua volta, invece, il Tribunale di Bologna (sentenza 16 maggio 2006) ha provato a chiarire quali sono i tabù industriali che gli articoli 98 e 99 del Codice della proprietà industriale mirano a proteggere. «La definizione di segreto di cui alla normativa citata - spiegano i magistrati - deve coincidere con la nozione di know-how». E cioè quella serie «di informazioni riservate necessarie o uti-

### LENTEZZE IN AULA

La Corte Costituzionale ha stabilito che alla materia non venga applicato il rito societario, più rapido di quello ordinario

li per condurre adeguatamente un processo produttivo o distributivo (o organizzativo comune di attività economica), il cui valore economico è dato dal risparmio e dal conseguente vantaggio realizzato con la sua utilizzazione».

### Quanto segreti

Il livello di riservatezza - ed è questo il vero problema interpretativo - resta una questione di punti di vista. Come spiega il Tribunale di Catania (sentenza 10 ottobre 2005), «la nozione di segretezza delle conoscenze aziendali deve essere intesa in senso relativo, giacché, ove la si interpretasse in senso assoluto, si coliderebbe col dato di fatto che certi collaboratori si trovino a conoscere informazioni aziendali che devono rimanere strettamente riservate». Insomma, non c'è nulla di oggettiva-

mente indivulgabile. Di sicuro, però, commette il reato di rivelazione di segreti industriali, al pari di un ex dipendente, il professionista che si appropria di notizie alle quali accede per lavoro. Ha avuto modo di spiegarlo addirittura la Cassazione penale (sentenza 25174/05) che ha condannato il legale rappresentante di una società, colpevole di aver "copiato" il progetto di un dispositivo di filtraggio top secret di un'azienda con la quale aveva avuto una collaborazione, per poi costruire e commercializzare l'apparecchio.

### Che tipo di processo

Infine, grazie alla Corte costituzionale (sentenza 170/2007) si sa che alle cause sulla violazione di segreti industriali non si applica il rito societario, considerato più veloce di quello ordinario.

## Ambiente. La gestione del mare A Cagliari il Coast day

CAGLIARI

Alla Manifattura Tabacchi di Cagliari si svolge oggi la giornata conclusiva della Settimana delle coste sarde promossa dalla Regione Sardegna e dall'International Marine Center Onlus.

Un incontro tra le istituzioni regionali che si occupano di ambiente e turismo, centri di ricerca, associazioni e organismi internazionali con il fine di promuovere la conoscenza, il rispetto delle coste e il turismo sostenibile. L'avvenimento rientra nella campagna internazionale per la protezione e la conservazione delle coste finanziata dall'Unione europea e della Banca mondiale. Oltre all'Italia con la Sardegna, i Paesi coinvolti nel Coast Day sono: Algeria, Croazia, Cipro, Egitto, Francia, Grecia, Giordania, Libano, Montenegro, Marocco, Autorità Palestinese, Spagna, Siria, Tunisia, Turchia.

confronto tra scienziati, intellettuali e scrittori a cui seguirà uno scambio di esperienze con le associazioni impegnate nella salvaguardia ambientale. Tra gli altri partecipano il presidente di Italia Nostra, Giovanni Lo Savio, il presidente del Fai, Giulia Maria Crespi, Rosalba Giugni di Marevivo e Marco Costantini di Wwf Italia. Lo spazio dedicato al dibattito sarà chiuso dalla tavola rotonda sui Governi del mare con il presidente sardo Renato Soru e il ministro dell'Ambiente algerino, Sherif Rahmani.

La Settimana delle coste sarde è un evento a emissioni zero. La produzione di anidride carbonica sarà azzerata grazie all'intervento della società Azzero Co2. Per neutralizzare l'inquinamento si provvederà all'acquisto di 36 crediti di emissione sul mercato volontario, ovvero alla piantumazione di 36 alberi.

## Vendite per posta. I piani della società Otto si rafforza in Italia

Vincenzo Chierchia

MILANO

Il gruppo tedesco Otto rafforza le attività in Italia nel business della vendita per corrispondenza e diventa leader di mercato. La controllata Bon prix, attiva sul mercato italiano dal 1997, ha rilevato di recente la Euronova anch'essa controllata dal gruppo Otto. Dalla fusione delle due realtà nasce un polo da oltre cento milioni di euro di fatturato con un tasso di crescita del 25% l'anno.

Oltre un milione in totale i clienti che utilizzano servizi per corrispondenza. Circa 250 gli addetti interessati dall'operazione di riassetto delle attività in Italia di un gruppo, Otto, che è presente in una ventina di Paesi con un centinaio di realtà. La fusione tra Bon prix, che si occupa prevalentemente di

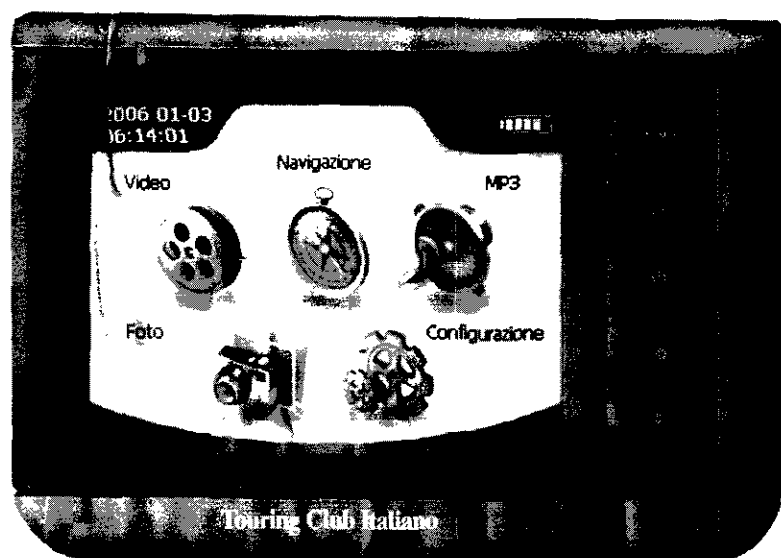
abbigliamento, con Euronova (prodotti per la casa), è stata accompagnata dal decollo di una altra realtà, la Get a line, che opera sempre nell'ambito del gruppo Otto.

E nei prossimi mesi la presenza del gruppo tedesco potrebbe aumentare ancora. È infatti in fase di valutazione lo sbarco in Italia della controllata Hermes, che si occupa di logistica e distribuzione di pacchi, particolarmente attiva in Germania. L'ingresso in grande stile di Hermes in Italia è legato all'evoluzione degli accordi tra Otto e Poste italiane, ma ha già rilevato una piccola società di consegne a Milano per gettare le basi del business nel nostro Paese. In fase di valutazione c'è poi anche lo sviluppo nel nostro mercato di una controllata Otto che si occupa di servizi finanziari.

### L'OFFERTA DELLA SETTIMANA DI SHOPPING24.IT

## NAVIGATORE TOURING CLUB ITALIANO

Non è un semplice navigatore, ma una vera guida multimediale per i tuoi viaggi! Ha tutte le funzioni dei navigatori di fascia alta con istruzioni vocali. Ma ci sono cose che soltanto il T-370 del Touring Club Italiano ti dà: decine d'itinerari consigliati dal TCI, tutte le notizie turistico-culturali anche a voce, centinaia di fotografie per riconoscere i luoghi, l'indicazione di alberghi, ristoranti, negozi, musei e servizi. Se sei in autostrada, ti segnala stazioni di servizio, distanze e tempi per arrivarci, attrazioni e itinerari più interessanti nelle vicinanze. Dotato di display touch-screen LCD da 3.5 pollici, può riprodurre mp3 e filmati e visualizzare foto. Inclusi nella confezione: caricatore da muro e per auto, auricolare, supporto a ventosa, cavo USB. Garanzia 24 mesi.



a soli  
**€ 179,00**  
anzichè € 349,00

Navigatore Touring  
codice SL - 33194

### COME ORDINARE

per telefono

Numero Verde  
**800-911224**

Numero verde GRATIS  
attivo 7 giorni su 7  
dalle 9 alle 21

su internet

www.shopping24.it

COME PAGARE  
in contrassegno  
o con carta di credito

Spese di spedizione: € 5,46

Gestito da bow.it

SHOPPING  
24.it