

# LA MINACCIA INTERNA

## UNA DISASTROSA PERDITA DI DATI

Uno studio europeo sul pericolo di perdere i dati che corrono le aziende a causa dei loro dipendenti

EXECUTIVE SUMMARY

INTRODUZIONE

CAPITOLO 1  
DATI IN MOVIMENTO

CAPITOLO 2  
PERDITA DEI DATI: LA  
DIMENSIONE DEL  
PROBLEMA

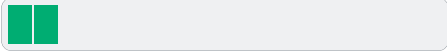
CAPITOLO 3  
SOTTO CONTROLLO

CAPITOLO 4  
LA PICCOLA VIA DI FUGA  
DELLA SICUREZZA

CAPITOLO 5  
I COSTI DERIVANTI DALLA  
PERDITA DI DATI

CAPITOLO 6  
COSA POSSONO FARE LE  
AZIENDE PER PROTEGGERSI





L'idea tradizionale legata alle minacce per la sicurezza dell'azienda è che esse abbiano origine dall'esterno. Poiché l'ambiente delle minacce evolve e diventa sempre più sofisticato, le aziende effettuano significativi investimenti in contromisure per difendersi, tra cui anti-virus, anti-spam, firewall e sistemi di intrusion prevention (per nominarne solo alcuni) – il tutto nel tentativo di bloccare malware e intrusi che cercano di penetrare nella loro rete aziendale.

Comunque, molti non riescono a vedere la propria strategia di sicurezza nel senso inverso ovvero rispetto all'incombente minaccia interna. Ma, in modo intenzionale o accidentale, oggi la forza lavoro rappresenta una minaccia alla sicurezza sempre più seria per le aziende, che ha la potenzialità di danneggiare il brand di un'azienda, la sua reputazione e l'azienda stessa.

La 'perdita di dati' è stata proclamata quale uno dei problemi più incalzanti per le aziende nel 2007 e Gartner ha inoltre recentemente affermato che ci troviamo nel mezzo di 'un'epidemia di perdita di dati' \*. La maggior parte di tutte le informazioni aziendali ora sono in formato elettronico, molte di queste sono accessibili a qualsiasi dipendente o collaboratore, e non è quindi difficile comprendere come la perdita dei dati rappresenti un disastro in attesa di verificarsi.

Mentre la maggior parte delle aziende analizza le email in entrata in caso di contenuti non richiesti, molti non controllano le loro mail interne e in uscita consentendo

il trasferimento non autorizzato di dati all'interno o al di fuori dell'azienda. Il crescente uso di dispositivi portatili da parte dei dipendenti mette a rischio l'integrità e la sicurezza degli asset digitali. Laptop aziendali, memorie USB, telefoni cellulari e iPod permettono agli impiegati di trasportare facilmente varie migliaia di documenti in una volta sola al di fuori dei parametri aziendali, e ancora la maggior parte di questi dispositivi è al di fuori del controllo dei dipartimenti IT.

Infatti, quasi otto su 10 grandi istituzioni finanziarie hanno subito una violazione di sicurezza negli anni passati e varie migliaia di più non sono state segnalate. Le implicazioni finanziarie e di business derivanti dalla perdita di dati possono essere catastrofiche, ma tali infrazioni possono lasciare le aziende e i loro responsabili legalmente esposti alla violazione delle leggi sulla privacy o non aver rispettato gli obblighi di corporate governance.

Dodici mesi fa, nel report 'La minaccia dall'interno', abbiamo evidenziato quanto i dipendenti mettano inconsapevolmente a rischio le loro aziende collegando sistemi 'non verificati' sulla rete aziendale. In questo report continuiamo a esaminare la portata della minaccia rappresentata dalla perdita di dati che le aziende europee devono affrontare da parte dei propri dipendenti e suggeriamo le best practice per affrontare la minaccia interna faccia a faccia.

**MIKE DALTON, PRESIDENTE, MCAFEE EMEA**



\* Gartner, 'Gartner Identifies Top 5 Steps to Dramatically Limit Data Loss and Information Leaks', 7 Agosto 2006  
<http://www.gartner.com/it/page.jsp?id=495173>

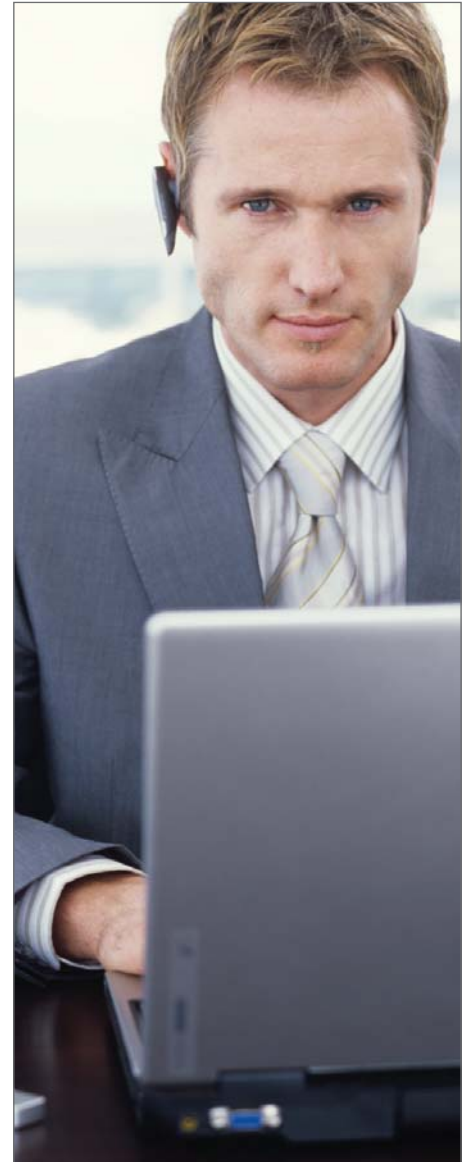


McAfee ha commissionato la ricerca in sei nazioni in Europa, tra 600 impiegati. \* Lo scopo è quello di comprendere i danni all'organizzazione causati dalla perdita dei dati e il livello cui i dipendenti mettono a rischio i dati aziendali più importanti.

La ricerca ha evidenziato che la gestione spesso indolente di dati riservati da parte dei dipendenti è una preoccupazione seria per la sicurezza e la maggioranza delle aziende europee non sta adottando le misure necessarie per salvaguardare i propri asset contro i rischi della perdita dei dati.

### I PRINCIPALI RISULTATI INCLUDONO:

- » In media, 11 documenti riservati vengono portati fuori dagli uffici europei ogni settimana su dispositivi portatili
- » Il 37% delle aziende europee non dispone di una serie di policy per gestire i documenti più importanti e, laddove le policy esistano, il 24% dei dipendenti non le conosce
- » Il 52% dei dipendenti europei porterebbe con sé i dati aziendali al momento di andarsene
- » I documenti interni di ogni giorno e i dati dei clienti sono due delle tipologie di documenti più comuni che vengono portati al di fuori dell'azienda in modo elettronico o fisico. Seguono le informazioni finanziarie dell'azienda
- » I dipendenti utilizzano sempre più dispositivi portatili, inclusi memory stick e telefoni cellulari per rimuovere dati riservati dalle loro aziende
- » I servizi di posta elettronica Web e anche l'IM vengono utilizzati per trasferire informazioni confidenziali fuori dall'azienda



Il palese movimento incontrollato di informazioni confidenziali dentro e al di fuori delle aziende evidenzia come i dipendenti rappresentino sempre più una minaccia interna per la sicurezza e l'integrità dell'azienda.

Le abitudini aziendali sono molto cambiate negli ultimi decenni. La presenza e l'utilizzo quotidiano di internet nelle nostre vite lavorative ha portato a un miglioramento della rapidità dei processi e delle comunicazioni aziendali e ciò significa che i dipendenti lavorano più velocemente, in modo più intelligente e spesso anche più ore di quanto accadesse prima.

Altri importanti miglioramenti nelle abitudini che hanno aumentato le opportunità di business e la redditività, ma anche potenzialmente esposto le aziende a un maggior rischio di sicurezza includono:

#### COLLABORAZIONE INTERNA:

Le aziende operano sempre più all'interno di mercati globali. Le nazioni commerciano informazioni e risorse, uffici satellite si collegano tra fusi orari differenti e dirigenti e altri dipendenti collezionano sempre più chilometri per visitare filiali, partner, clienti esistenti e potenziali.

- » **Il punto di vista dell'azienda:** Le collaborazioni internazionali aprono nuovi mercati e opportunità. La capacità di reagire immediatamente alle indicazioni del mercato e alle esigenze e richieste di business interne ed esterne favoriscono maggior competitività e collaborazione.
- » **Lo sforzo per la sicurezza:** Operare in continenti e fusi orari differenti ha portato a affidarsi sempre più all'invio fisico dei dati o allo scambio elettronico degli stessi. Ciò porta a un crescente rischio di intercettazione o perdita durante il tragitto.

#### IL CRESCENTE NUMERO DI COLLEGAMENTI CON PARTNER, FORNITORI E TERZE PARTI:

Le aziende stanno ampliando i propri confini per trarre vantaggio da risorse e competenze fornite da partner, sub-contraenti esterni e terze parti.

- » **Il punto di vista dell'azienda:** I partner forniscono idee, competenze e fondi per completare le attuali prassi. L'outsourcing permette una gestione dei costi efficiente e innovazione.
- » **Lo sforzo per la sicurezza:** Lo scambio di informazioni può esporre al rischio le informazioni stesse. Più la 'rete' è estesa, più è probabile che le informazioni possano diffondersi e che il controllo dei dati sia meno accurato.

#### FLESSIBILITA' NEL MODO DI LAVORARE:

Un numero crescente di lavoratori sceglie la flessibilità offerta dal lavorare da casa che molte aziende oggi offrono. Gartner prevede che nel 2007 ci saranno oltre 60 milioni di telelavoratori in tutto il mondo.

- » **Il punto di vista dell'azienda:** Fornire a una forza lavoro mobile l'accesso alle informazioni di cui hanno bisogno esattamente dove e quando ne hanno bisogno, permette di migliorare l'efficienza e la produttività del dipendente.
- » **Lo sforzo per la sicurezza:** Una forza lavoro sempre più in movimento significa un numero maggiore di dati in movimento. Informazioni riservate vengono costantemente trasferite tra le reti per agevolare il lavoro quando si è in viaggio, aumentando il rischio che vengano perse, rubate o danneggiate.

TUTTI QUESTI FATTORI HANNO PORTATO A UN AMBIENTE DI BUSINESS IN CUI LA CONDIVISIONE DELLE INFORMAZIONI E' DIVENTATA UNA PRATICA STANDARD, SE NON OBBLIGATORIA, MA ANCHE UNA PRATICA CON CUI LE POLICY DI SICUREZZA SPESSO NON SONO RIUSCITE A STARE AL PASSO.

COME RISULTATO DI QUESTO MOVIMENTO GLOBALE DI INFORMAZIONI, LE AZIENDE SI TROVANO AD AFFRONTARE IL CRESCENTE PROBLEMA DELLA FUGA DEI DATI.

In base alla nostra ricerca, l'impiegato medio europeo preleva o trasferisce 11 documenti riservati al di fuori della sua azienda settimanalmente. I dipendenti olandesi sono i peggiori con 19 documenti riservati che lasciano i confini dell'azienda ogni settimana, seguiti dagli Spagnoli che ne rimuovono 13. Gli Inglesi sembrano essere i più consapevoli per quanto riguarda la riservatezza, condividendo una media di sei documenti alla settimana.

#### NUMERO MEDIO DI DOCUMENTI AZIENDALI \* PORTATI FUORI DALL'AZIENDA PER DIPENDENTE OGNI SETTIMANA

MEDIA EUROPEA: 11

INGHILTERRA	FRANCIA	GERMANIA	ITALIA	OLANDA	SPAGNA
6	12	8	11	19	13



Piani societari, informazioni finanziarie, documentazione relativa ai dipendenti, dati dei clienti e contratti legali vengono tutti messi a rischio dalle azioni dei lavoratori europei. In modo preoccupante, circa un terzo (31%) degli intervistati inviano informazioni finanziarie aziendali ad altri al di fuori dell'azienda come parte della loro routine quotidiana, mentre il 20% inoltra anche contratti legali.

#### TIPO DI DOCUMENTI REGOLARMENTE INOLTTRATI AL DI FUORI DELL'AZIENDA (%)

	INGHILTERRA	FRANCIA	GERMANIA	ITALIA	OLANDA	SPAGNA
PIANI DI BUSINESS DELL'AZIENDA	24	23	15	6	15	15
INFORMAZIONI FINANZIARIE	39	22	13	31	41	40
DATI DEI CLIENTI	50	36	36	32	50	32
INFORMAZIONI SUL DIPENDENTE	24	10	16	21	31	12
CONTRATTI LEGALI	25	28	11	22	19	16

\* Con 'Documenti aziendali' si fa riferimento a piani aziendali, informazioni finanziarie, dati del cliente, documenti interni, dettagli dei fornitori, informazioni sul dipendente e contratti legali

**LA PRIVACY DEI DIPENDENTI VIENE FACILMENTE VIOLATA POICHÉ UN QUINTO (19%) CONDIVIDE I PROPRI DETTAGLI CON CONTATTI ESTERNI E, MENTRE IL 92% AMMETTE CHE LA GESTIONE SICURA DI DOCUMENTI RISERVATI E' CRUCIALE PER MANTENERE LE RELAZIONI CON I CLIENTI, IL 39% INOLTRA SENZA DIFFICOLTÁ DATI E DOCUMENTI DEI CLIENTI AD ALTRI AL DI FUORI DELL'AZIENDA.**

Ancora, nonostante questa evidente e crescente condivisione di informazioni, le aziende sembrano riluttanti a intraprendere le azioni opportune per educare i dipendenti – e essenzialmente per proteggere sé stessi da violazioni ai dati e dalle potenziali conseguenze catastrofiche associate. Oltre un terzo delle aziende europee (37%) non dispone di policy per gestire i documenti riservati e, laddove le policy esistono, quasi un quarto (24%) dei dipendenti non le conosce.

#### LA VOSTRA AZIENDA DISPONE DI POLICY RELATIVE AL TRATTAMENTO DI INFORMAZIONI RISERVATE?

	INGHILTERRA	FRANCIA	GERMANIA	ITALIA	OLANDA	SPAGNA
SÌ	87	44	68	56	67	55
NO/ NON LO SO	13	56	32	44	33	45

#### CONOSCE LA POLICY?

	INGHILTERRA	FRANCIA	GERMANIA	ITALIA	OLANDA	SPAGNA
NON LO SO	28	34	19	27	22	16

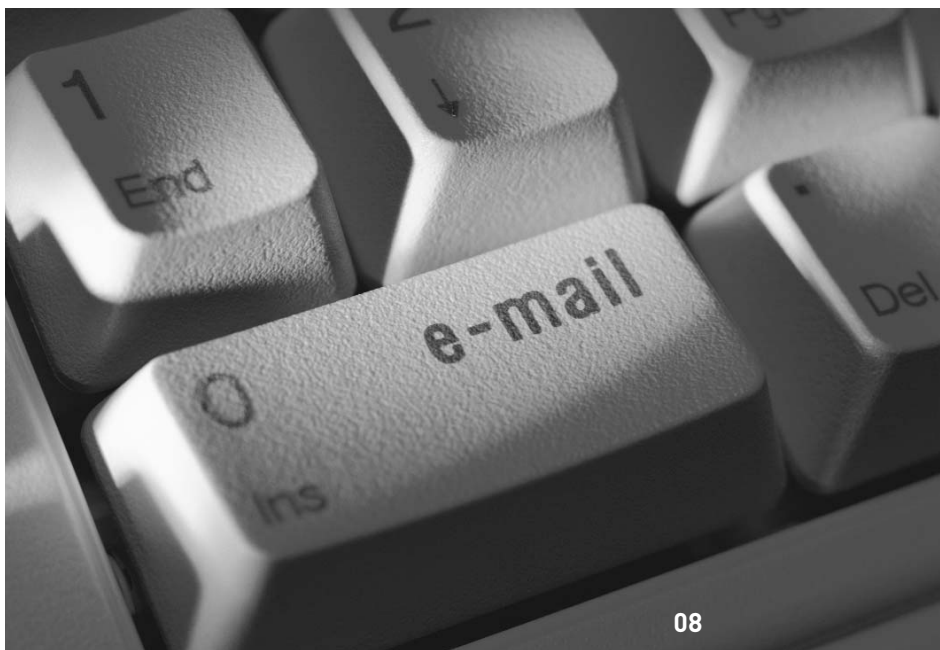
Al giorno d'oggi, le informazioni sono spesso l'asset più prezioso di un'azienda. Comunque, la ricerca di McAfee ha rivelato che i dati proprietari o i segreti aziendali sono spesso inoltrati tramite la rete o la posta elettronica, fuoriescono dall'azienda su un iPod o un drive USB o addirittura vengono consegnati documenti stampati direttamente a qualcuno di esterno. Mentre i dipartimenti IT sono sempre più concentrati sulla prevenzione di attacchi esterni, molti non riconoscono il rischio che le informazioni vengano trasferite liberamente al di fuori dell'azienda.

**Molti dipendenti utilizzano metodi che consentono loro di aggirare le misure di sicurezza. Un quarto (26%) di coloro che hanno inviato informazioni dei clienti al di fuori dell'azienda ammettono di utilizzare servizi di email web come Yahoo o Hotmail.**

### INSTANT MESSAGING

Circa un quarto (23%) di coloro che ammette di inviare documenti al di fuori dell'azienda ha utilizzato anche servizi di Instant Messenger (IM) per trasferire piani di business aziendali mentre uno su cinque (20%) ha inviato informazioni finanziarie aziendali e spreadsheet utilizzando IM.

L'IM fornisce ai dipendenti un modo veloce e meno strutturato di comunicare, ma laddove il suo utilizzo viene consentito non è per regolamentato. E' inoltre soggetto a una serie di ulteriori timori legati alla sicurezza. Non solo l'IM è stato recentemente utilizzato per diffondere botnet e worm (come la famiglia Mytob) ma gli utenti sono stati spinti a rivelare informazioni confidenziali da parte di criminali informatici utilizzando falsi account IM.



### LA CULTURA DELL'EMAIL

L'email aziendale è il mezzo più comune per inviare informazioni all'esterno con l'86% dei dipendenti europei che ammette di inoltrare regolarmente i documenti. Ancora, i dati possono essere inviati troppo facilmente a qualcuno di sbagliato, i dipendenti possono involontariamente inviare dati riservati a concorrenti e altri e gli utenti possono essere ingannati e portati a inviare informazioni a persone a cui non dovrebbero.

### CASE STUDY:

#### ERRORI TRAMITE L'EMAIL

**Una delle più grandi aziende di servizi finanziari indipendenti in Inghilterra ha inviato tre email a un totale di 2.600 dei propri clienti chiedendo loro di chiamare urgentemente l'helpline. Un errore ha fatto sì che ogni indirizzo fosse visibile a tutti coloro presenti nell'elenco, e la situazione è peggiorata quando i messaggi di risposta automatici di assenza hanno rivelato numeri di telefono diretti e di cellulari.**

**L'errore ha portato l'azienda all'infrazione delle leggi sulla protezione dei dati e a dover affrontare clienti indignati che erano stati esposti al rischio di frode. Oltre alle azioni legali che l'azienda avrebbe potuto affrontare, ha inoltre dovuto farsi carico dei risarcimenti.**

## IL BUON VECCHIO DOCUMENTO STAMPATO

Ancora, nonostante il crescente utilizzo di nuovi mezzi tecnologici per trasferire le informazioni, il tradizionale documento stampato mantiene il suo stato di principale potenziale vulnerabilità per l'azienda. I dipartimenti IT raramente hanno la capacità di monitorare e limitare cosa viene stampato o dove quest'informazione viene lasciata.

La ricerca mostra che il dipendente medio europeo stampa frequentemente informazioni finanziarie aziendali (83%), documenti dei clienti (83%) e contratti legali (87%). Il rischio che queste informazioni finiscano in mani sbagliate è ancor più complesso poiché oltre la metà (54%) degli impiegati non distrugge i documenti riservati e uno su dieci ammette di lasciare frequentemente le informazioni nel cassetto della stampante.

### TIPO DI DOCUMENTI STAMPATI REGOLARMENTE DAI DIPENDENTI (%)

	INGHILTERRA	FRANCIA	GERMANIA	ITALIA	OLANDA	SPAGNA
PIANI DI BUSINESS DELL'AZIENDA	83	74	87	100	73	80
INFORMAZIONI FINANZIARIE	82	82	85	90	78	85
DATI DEI CLIENTI	82	78	83	84	88	81
INFORMAZIONI SUL DIPENDENTE	88	60	56	100	87	75
CONTRATTI LEGALI	92	86	82	82	95	81



L'utilizzo incontrollato di dispositivi di storage portatili all'interno e fuori dalla rete aziendale crea un'importante falla nella sicurezza. I dispositivi di storage portatili sono sempre più diffusi, diventano più piccoli e più potenti con una maggiore capacità di storage. Tali dispositivi alimentano una cultura aziendale che spinge a portare con sé e trasferire grandi quantità di dati aziendali strategici quotidianamente.

La ricerca McAfee mostra che documenti riservati vengono comunemente portati al di fuori dell'azienda tramite dispositivi di

storage portatili, con quasi la metà degli impiegati europei che ammette di rimuovere documenti finanziari (45%), mentre un terzo trasferisce piani di business dell'azienda (38%) e dati dei clienti (34%).

Le chiavette USB rappresentano il dispositivo portatile più diffuso con oltre un quarto dei dipendenti (26%) che li utilizza regolarmente per rimuovere le informazioni. Comunque, invece di trattare questi dispositivi con cura, il 15% degli impiegati europei li ha prestati ad altri.

“Il rischio reale arriva da utenti non curanti che lasciano piccoli dispositivi portatili in posti dove non dovrebbero.”\*

Jeremy Green,  
Enterprise Mobility Analyst di Ovum

## IL FURTO DI DATI AZIENDALI

Di fatto, le aziende europee devono velocemente attrezzarsi per evitare che i dipendenti che lasciano l'azienda rubino dati aziendali con oltre la metà (52%) di quelli intervistati che confessano che porterebbero di sicuro con sé le informazioni e i documenti aziendali al momento di lasciare l'azienda. I dipendenti Francesi e Italiano sono i più propensi a portare furtivamente le informazioni fuori dall'edificio mentre i dipendenti Inglesi si ritengono i più degni di fiducia con il 70% che non ruberebbe mai dei dati.

## UN PICCOLO RISCHIO?

- » Un singolo drive flash USB può contenere fino a 8GB di informazioni
- » Una penna USB da 1GB può contenere oltre 536.000 documenti dei clienti
- » Un player MP3 da 20GB può contenere oltre 750.000 documenti
- » Un iPod da 60GB iPod può contenere oltre 660 file da 90MB



## CASE STUDY: LA MEMORIA USB DISPERSA

Nel Gennaio 2007, la cronaca ha riportato che un ufficiale del Ministro degli Esteri olandesi si è dimenticato una chiavetta di memoria contenente informazioni confidenziali non cifrate in un autonoleggio. Il dispositivo smarrito conteneva codici d'ingresso segreti della casa di un diplomatico olandese e i nomi delle guardie che accompagnarono il Primo Ministro in un recente viaggio in Polonia. Conteneva inoltre dettagli sull'ambasciata olandese, come mappe e libri contabili oltre a lettere di rifiuto indirizzati a candidati che includevano foto e numeri di telefono.

Anche degli ufficiali del Ministro della Difesa Olandese hanno recentemente smarrito delle chiavette USB. Una che conteneva informazioni sulla missione militare olandese nella provincia afgana di Uruzgan venne poi ritrovata in una macchina noleggiata.

Questi esempi dimostrano come questi dispositivi portatili compatti, in grado di contenere enormi quantità di dati, possono facilmente mettere a repentaglio l'integrità delle informazioni aziendali.

\* <http://mobile.vnunet.com/computing/analysis/2172239/upwardly-mobile>



La sicurezza una volta era vista come un'opzione – oggi non è più così. Il riconoscimento del significato strategico e economico dell'integrità delle informazioni sta attirando l'attenzione dei responsabili di aziende, associazioni industriali, enti di vigilanza nazionali e dell'Unione Europea.

In realtà, i principali scandali aziendali come quelli di Enron e WorldCom hanno portato a cambiamenti legislativi e regolatori creati per proteggere gli investitori e migliorare la corporate governance.

Alcune leggi, inclusi l'Accordo Basilea II, il Data Protection Act, la Gramm-Leach -Bliley, l'Health Insurance Portability and Accountability Act (HIPAA), la Sarbanes Oxley Act (SOX) e l'Ottava direttiva dell'Unione europea che è in fase di sviluppo, ora rendono le aziende responsabili di governance, privacy e protezione dei dati.

La pressione della conformità normativa significa che le aziende sono sempre più responsabili per la negligenza dei loro dipendenti o il trattamento imprudente di informazioni riservate. Le aziende non solo devono affrontare i costi diretti legati alla perdita di informazioni ma anche i costi indiretti.

L'FBI ritiene che il costo complessivo di tutte le violazioni dei dati lo scorso anno, inclusi i dati aziendali, ammonti a un totale di 62.7 miliardi di dollari.\*

#### DIRETTI:

- » CAUSE IN TRIBUNALE
- » MULTE NORMATIVE
- » CALL CENTRE PER GESTIRE RECLAMI E RICHIESTE DEI CLIENTI

#### INDIRETTI:

- » PERDITA DI PROPRIETA' INTELLETTUALE
- » DANNI PER LA REPUTAZIONE
- » PERDITA DI VALORE DEL BRAND

**“Il costo del rischio per la reputazione è superiore a quello dei rischi finanziari” \*\***

Esperto di sicurezza in un'Associazione di Banchieri Europei

Questi costi indiretti cresceranno ancora di più in Europa nel prossimo futuro. Segnalare le violazioni dei dati personali è stato obbligatorio per due anni negli Stati Uniti con il risultato che i CIO sono estremamente consci di ogni occasione di vulnerabilità. Quando simili requisiti entreranno in vigore in Inghilterra alla fine di quest'anno si manifesterà una nuova dimensione del rischio per la reputazione.

**Si prevede che questo trend si estenderà a tutti i principali mercati.**

\* [www.internetnews.com/bus-news/article.php/3654211](http://www.internetnews.com/bus-news/article.php/3654211)

\*\*Rapporto McAfee sul rischio per la reputazione del 2006

## CASE STUDY: UNA CAUSA PER LA PERDITA DEI DATI

Gruppi di veterani hanno intentato una imponente causa rivendicando che l'U.S. Department of Veterans Affairs (VA) "non ha manifestatamente rispettato i diritti alla privacy praticamente di ogni uomo o donna che abbia indossato un'uniforme militare degli Stati Uniti," dopo che un laptop è stato rubato dalla casa di un dipendente.

Il laptop conteneva nomi, numeri di previdenza sociale e date di nascita di 26,5 milioni di veterani e alcuni consorti, oltre ad alcuni punteggi di invalidità. Nessuno dei dati era codificato. In base alla querela, il dipendente aveva abitualmente portato a casa informazioni personali per almeno tre anni.

La denuncia pretendeva che la corte chiedesse al VA di pubblicare la natura di ogni suo database contenente informazioni personali dei veterani, di rivelare quali informazioni contenessero e perché avessero bisogno di tali informazioni.

La denuncia richiedeva inoltre alla corte di proibire ai dipendenti del VA di rimuovere informazioni, o anche di portare iPod, chiavette di memoria, dispositivi USB e simili in ufficio.

I veterani del VA richiesero inoltre un risarcimento di 1.000 dollari per ogni persona elencata nei file del database mancante.



Alla luce dell'evoluzione dei requisiti legali e delle minacce tecnologiche per la sicurezza, è importante che le aziende instillino la sicurezza nella cultura della loro organizzazione.

Le aziende dovrebbe utilizzare, come minimo, una strategia di base per il risk management, creare policy e implementare tecnologia per salvaguardare i dati. Comunque, le policy combinate con la tecnologia focalizzate sugli attacchi esterni, da sole non sono chiaramente sufficienti per proteggere le aziende dalla minaccia della perdita dei dati. La cruda realtà è che i dati aziendali sensibili possono finire facilmente nelle mani sbagliate - deliberatamente o accidentalmente - a causa del comportamento del dipendente.

Per proteggere i dati, il brand e la reputazione dell'azienda dai danni derivanti dalla perdita dei dati, la miglior soluzione risiede nella combinazione di educazione del dipendente con un investimento intelligente in una soluzione completa per il security risk management.

**Di seguito alcuni punti che le aziende dovrebbero prendere in considerazione quando creano una strategia di sicurezza a 360°:**

### **Sviluppare, implementare e garantire conformità di una policy di sicurezza**

Il primo passo che le aziende dovrebbero intraprendere è quello di sviluppare una policy di sicurezza personalizzata per la propria azienda. Per esempio, un retailer dovrebbe consentire ai dipendenti di accedere con facilità ai dati, ma implementando stretti controlli per gestire cosa tali dipendenti possono e non possono fare con i dati cui hanno accesso.

### **Salvaguardare i dati a ogni livello**

Le aziende devono avere un approccio proattivo e prevedere tutti i possibili canali di fuoriuscita dei dati. Le aziende devono valutare gli attuali rischi per la sicurezza, le esigenze dipartimentali e l'utilizzo legittimo dei dispositivi.

### **Controllo e monitoraggio degli accessi**

Un controllo degli accessi adeguato per i dipendenti limita la possibilità di accedere a un particolare asset aziendale solo a coloro che richiedono accesso in occasioni particolari o esigenza specifica. Il monitoraggio fornisce al team di sicurezza un percorso e la comprensione della verifica degli schermi di accesso dei dipendenti.

### **Monitorare e prevenire l'installazione e l'utilizzo di applicazioni non autorizzate**

E' importante fornire ai dipendenti policy e procedure dettagliate su come utilizzare in modo sicuro la tecnologia al di fuori dell'ufficio.

Comunque, non ha molto senso avere una policy per le informazioni confidenziali se i dipendenti non vengono informati delle procedure e dei rischi corsi dall'azienda se tali passaggi non vengono rispettati.

### **Educare e (ri) formare i dipendenti**

Formazione e gestione complete sulle policy e le procedure di sicurezza dell'azienda sono due elementi critici. I dipendenti possono aiutare le aziende per quanto riguarda i requisiti di conformità e a costituire un'importante linea di difesa contro le minacce che arrivano dall'interno e dall'esterno. Dovrebbero essere formati in base alle responsabilità e requisiti quotidiani per accedere e proteggere i dati sensibili. I dipendenti possono diventare delle risorse preziose per la sicurezza.

## SOLUZIONI TECNOLOGICHE

**“Per potersi difendere con successo contro la fuoriuscita di informazioni, i prodotti devono risiedere sul desktop di coloro che hanno accesso a informazioni estremamente riservate e controllare quanto segue: trasferimento di file a e da periferiche come i drive USB; copia e incolla di informazioni tra le applicazioni; e l’utilizzo di canali di output come stampanti e fax. Il contesto, oltre al contenuto, è fondamentale per l’analisi e la classificazione – e per comprendere il contesto è necessario un agent desktop.”\***

Forrester Research, Dicembre 2006

Il security risk management è un approccio che integra la protezione contro le minacce con la conformità. Il componente tecnologico di un approccio esaustivo al security risk management deve includere funzionalità di prevenzione delle minacce come anti-virus, intrusion prevention, anti-spyware, integrate con funzioni di gestione della conformità come policy enforcement, remediation delle vulnerabilità, controllo degli accessi alla rete e funzionalità di audit.

Mentre la maggior parte delle soluzioni DLP (soluzioni gateway-based) prevengono il trasferimento non autorizzato di dati sensibili via e-mail e Internet, queste

soluzioni non monitorano le attività sul desktop. Le organizzazioni devono implementare una soluzione DLP (soluzione host-based) che controlla la minaccia interna da entrambi i punti di vista. Questa soluzione deve offrire protezione universale, anche per drive USB e laptop, per migliorare il controllo delle attività dei terminali. Un altro requisito fondamentale è il controllo content-aware, per prevenire perdite monitorando come i dati vengono consultati, creati e manipolati. Anche i dati che vengono copiati, incollati, compressi o codificati devono essere protetti – senza interrompere le attività lavorative quotidiane.

**IL RISULTATO FINALE E' CHE IN MODO INTENZIONALE O MENO, IL COMPORTAMENTO DEI DIPENDENTI PUÒ RAPPRESENTARE UNA MINACCIA SERIA E LEGITTIMA PER LA SICUREZZA AZIENDALE, PERCIO' LE ORGANIZZAZIONI DEVONO IMPLEMENTARE DELLE MISURE PROTETTIVE PER GARANTIRE UNA COPERTURA COMPLETA, AFFIDABILE E VERIFICABILE. SOLO IN QUESTO MODO LE AZIENDE POSSONO ESSERE CONFORMI ALLE NORMATIVE GOVERNATIVE, PROTEGGERE DATI PREZIOSI E MANTENERE INTATTA LA PROPRIA REPUTAZIONE.**

\* The Forrester Wave™: Information Leak Prevention, Q4 2006, 15 Dicembre, 2006, di Jonathan Penn e Thomas Raschke