



# 2. ■ Serie Business Advisor

Non mettete a rischio la vostra azienda

Come garantire che il software disponga di una licenza

## Quali rischi corre la vostra azienda?

Nel 2007, Business Software Alliance (BSA) ha chiesto all'organizzazione indipendente specializzata in ricerche di mercato GfK NOP di analizzare gli atteggiamenti delle piccole e medie imprese (PMI) europee nei confronti del software e la loro consapevolezza dei rischi legati all'uso di software senza licenza (comprese le copie contraffatte). I risultati hanno rivelato che il 95% delle PMI è "sicura" di avere la licenza completa per tutti i software installati. Tuttavia, un'indagine approfondita effettuata da IDC rivela che la pirateria del software è ancora molto diffusa in Europa, con picchi del 34% nell'Europa occidentale e del 51% in Italia.

Questa differenza tra la situazione percepita e quella reale suggerisce una mancanza di conoscenza dei dirigenti aziendali per quanto riguarda il software e la sua gestione. Si tratta di una situazione pericolosa. Il software è diventato rapidamente una delle risorse aziendali più preziose e critiche. Se le aziende non investono in risorse software e non le gestiscono e proteggono in modo adeguato, si espongono a numerosi rischi che possono avere rilevanti implicazioni finanziarie.

Business Software Alliance ha realizzato questa guida per evidenziare i reali rischi derivanti dall'uso di software senza licenza (software pirata, con licenze non valide o installato in più copie di quanto previsto dalla licenza) e i modi per proteggere la propria azienda e massimizzare i vantaggi ottenuti dal software in uso.

### Definizioni:

**Software senza licenza:** qualsiasi prodotto software installato su un PC senza che il contratto di licenza permetta o supporti tale installazione o senza la stipulazione di un contratto di licenza o di utilizzo con il detentore del copyright. Nel presente documento, il termine "software senza licenza" viene utilizzato per indicare tutte le tre forme di violazione del copyright del software riportate di seguito.

**Software underlicensed:** software installato su un numero di PC maggiore di quello consentito dal contratto di licenza. Per esempio, una licenza potrebbe consentire l'installazione del software su 20 PC. Se il software venisse installato su 30 PC, le 10 installazioni in più verrebbero considerate "senza licenza".

**Software mislicensed:** software utilizzato per scopi non consentiti dal contratto di licenza, come un software concesso in licenza per un utilizzo accademico ma che viene utilizzato per scopi commerciali.

**Software pirata:** software deliberatamente copiato (su vasta scala) per truffare i detentori del copyright con la distribuzione illegale tramite CD o siti Internet di download. È compreso in questa voce il "software contraffatto".

## Prefazione

Per molte PMI l'aspetto della gestione dei rischi sta cambiando rapidamente, con maggiore attenzione sull'amministrazione e la trasparenza e un apparentemente inarrestabile passaggio a regolamenti più rigidi. Molte aziende vengono tempestate da un flusso costante di messaggi che le invitano a migliorare nella gestione dei rischi. Ma quali sono i vantaggi per l'azienda? E perché si dovrebbe prestare attenzione ad aspetti della gestione dei rischi come la gestione delle risorse software e la sicurezza delle informazioni?

Le PMI costituiscono la maggioranza delle aziende di tutto il mondo. In Europa producono oltre la metà della ricchezza generata ogni anno e impiegano la grande maggioranza di forza lavoro di gran parte dei Paesi. La riluttanza a riconoscere o a prepararsi a una significativa interruzione dell'attività rende molte aziende potenzialmente vulnerabili anche alle minime interruzioni, mettendo a rischio, nel complesso, decine di migliaia di posti di lavoro e le tante altre aziende con cui collaborano, come fornitori o clienti.

I dirigenti delle PMI sono abituati ad affrontare problemi aziendali relativi alla modifica dei prezzi di fornitura, a nuovi concorrenti e a clienti esigenti. La dimestichezza con queste sfide quotidiane potrebbe generare un eccesso di sicurezza per quanto riguarda la capacità dell'azienda di fronteggiare i disastri, anche su scala ridotta.

Potrebbe essere sottovalutata anche l'incidenza totale di un'interruzione lavorativa. Uno studio condotto da Gartner rivela che il 40% delle aziende fallisce entro i cinque anni successivi a una grave interruzione delle attività lavorative. Da uno studio separato emerge che le aziende che impiegano più di trenta giorni a ripristinare la normale attività lavorativa sono esposte a un notevole rischio di cessazione dell'attività.

**Considerata l'attuale maggiore consapevolezza della vulnerabilità, è incredibile che così tante aziende siano impreparate a un'interruzione dell'attività. Questo fatto è ampiamente riconosciuto, ma raramente ne vengono affrontati i motivi.**

La nostra ricerca all'Henley rivela che un fattore importante nelle società che decidono di investire in attività di gestione dei rischi è l'influenza percepita delle fonti di minaccia rispetto alla propensione al rischio dell'azienda. Tuttavia, come sanno bene tutti i dirigenti senior delle PMI, i profitti sono la ricompensa di un'adeguata assunzione di rischi commerciali. Il rischio aziendale, in quanto componente fondamentale del profitto, è inevitabile.

La gestione dei rischi non riguarda semplicemente la riduzione del rischio. Riguarda anche la conoscenza della propensione al rischio dell'azienda e la limitazione dei rischi stessi, riducendo per quanto possibile la loro probabilità di presentarsi e/o il loro effetto senza frenare l'attività dell'azienda. Con una gestione ottimale dei rischi, l'azienda può tollerare una maggiore esposizione, aumentando i potenziali profitti senza però superare il livello accettabile di rischio. Una valida gestione dei rischi migliora la capacità di ripresa dell'azienda.

Molte aziende non riconoscono il ruolo del rischio nelle loro attività lavorative. Le aziende di maggiori dimensioni hanno un approccio strutturato all'investimento in nuovi progetti, traducendo il rischio in aspettative di rendimento. Tuttavia, le aziende più piccole potrebbero non applicare sempre tali metodi rigidi, esponendosi eccessivamente al rischio durante la crescita.

## **Che si tratti del risultato dell'interesse dell'amministratore delegato per il flusso di cassa o del tentativo di espansione, le aziende più piccole potrebbero mettere a rischio la sopravvivenza dell'intera attività espandendosi senza considerare la gestione del rischio.**

Questa situazione sta incidendo sulla gestione dei rischi legati alla sicurezza delle informazioni e il quadro si complicherà ulteriormente nell'immediato futuro con la nascita di nuove tecnologie. Lo sviluppo e l'implementazione di nuovi tipi di dispositivi informatici e di distribuzione del software incideranno notevolmente sui requisiti necessari degli approcci di valutazione dei rischi.

Ultimo ma non meno importante, non dovremmo dimenticare che sono i rischi percepiti direttamente che vengono affrontati con giudizio (rischi come l'attraversamento della strada). Purtroppo, troppi rischi legati al software vengono ancora considerati "virtuali". Molti dirigenti di PMI si saranno trovati di fronte a un disco rigido mal funzionante o a un virus sul computer, ma pochi avranno dovuto affrontare conseguenze molto gravi. Nonostante siano poche le grandi catastrofi aziendali legate al software, eventi di questo genere si sono verificati sia in grandi che in piccole organizzazioni.

Le implicazioni legali dell'utilizzo di software senza licenza possono essere notevoli, ma ciò che probabilmente è meno noto è che l'uso di software con licenza permette l'accesso all'assistenza tecnica e offre maggiore protezione contro virus o malware, con una conseguente riduzione delle interruzioni. In una realtà in cui la continuità lavorativa è fondamentale, le PMI sono meno in grado di superare i problemi derivanti da interruzioni lavorative rispetto alle aziende più grandi. Generalmente non hanno la stessa capacità di ripresa delle grandi organizzazioni che possiedono varie sedi, fondi accantonati e consulenti esterni. Come dimostrano la ricerca e i consigli qui presentati, spesso sono le piccole aziende che si espandono rapidamente a non prestare sufficiente attenzione alle importanti attività di gestione dei rischi come i controlli delle licenze software. Sono quindi esse le più vulnerabili.

Come viene detto in questa guida, il riconoscimento di questa maggiore vulnerabilità sembra scarso vista la mancanza di attività e preparazione. Che cosa possiamo fare a riguardo? E che cosa dovremmo fare? Dobbiamo essere più aperti per quanto riguarda le conseguenze di una inadeguata gestione dei rischi e i vantaggi di una buona gestione.

Troppo spesso nascondiamo i problemi per paura che possano influire negativamente sulla nostra reputazione. Soltanto comunicando tra noi possiamo sviluppare efficaci strategie di gestione dei rischi che rivolgano la giusta attenzione alle poche attività di gestione dei rischi davvero importanti, e che ci garantiscano di poter continuare a raccogliere i frutti della corretta assunzione dei rischi commerciali e a evitare le insidie di un'avventata assunzione dei rischi.

Questa guida aiuta in questo tentativo di comunicazione.

Per quanto riguarda le licenze software, l'equazione rischio-vantaggio è molto semplice.

I vantaggi operativi e "di reputazione" legati all'uso di software con licenze complete sono notevoli. I vantaggi dell'uso di licenze inadeguate non soltanto sono scarsi, ma sono ingestibili e fonte di rischi persino maggiori.

**Jean-Noel Ezingear,**  
**Henley Management School.**



## Software e rischio aziendale

Il software costituisce una delle risorse più preziose di un'azienda; da una recente ricerca commissionata da Business Software Alliance è emerso che il 94% delle aziende europee considera l'IT fondamentale per un'attività aziendale di successo<sup>1</sup>. Il software specializzato consente alle imprese di architetti, ingegneri, ricercatori e designer e alle organizzazioni finanziarie di essere competitive e sempre all'avanguardia. Anche nelle attività lavorative quotidiane, quasi tutte le aziende utilizzano fogli di calcolo per gestire le attività finanziarie, database per archiviare informazioni fondamentali, posta elettronica per comunicare (con colleghi, clienti e fornitori) e pacchetti di desktop publishing per creare presentazioni e materiale legato al marketing.

Può quindi risultare strano che il 51% del software nelle aziende italiane venga utilizzato senza una regolare licenza.<sup>2</sup>

La mancata conoscenza dello stato delle licenze software all'interno di una società non offre alcuna difesa, quindi è fondamentale che le aziende siano pienamente consapevoli dei rischi legati alla pirateria del software a cui vanno incontro e delle misure che possono adottare per evitare tali rischi ed essere quindi sicure di agire in modo legittimo.

Le aziende devono gestire i propri dipendenti in modo adeguato e rispettando determinati requisiti di legge, e lo stesso vale per il software che utilizzano. Molte aziende sono a conoscenza dei regolamenti finanziari e delle direttive in materia di gestione del personale, e attuano dei processi per rispettarli, ma hanno anche la responsabilità verso se stesse e verso gli azionisti o i proprietari dell'attenta gestione delle risorse software e della promozione di un livello adeguato di conoscenza all'interno dell'azienda.



<sup>1</sup> Fonte: ricerca sul rischio commerciale "Commercial Risk" condotta da GfK NOP, 2007

<sup>2</sup> Fonte: studio sulla pirateria del software "Software Piracy" condotto da IDC, 2007

Potrebbe sembrare complicato all'inizio, in particolare se l'azienda si espande rapidamente o se sono in corso notevoli cambiamenti alla struttura aziendale. Tuttavia, oltre a stabilire il metodo migliore per collaborare e comunicare con azionisti/proprietari e dipendenti, esaminare i potenziali cambiamenti da attuare allo stato finanziario e rivedere i contratti stipulati con fornitori e clienti, è necessario dedicare del tempo alla gestione dei requisiti software. A lungo termine il tempo impiegato risulterà ben speso.

Una gestione del software ben implementata non soltanto consente di evitare i rischi che può correre l'azienda a causa dell'uso di software senza licenza, ma può anche aumentarne l'efficienza e ridurre notevolmente i costi, non soltanto in termini di spese dirette per il software, ma anche di costi relativi a processi e infrastrutture.

I vantaggi di un'efficace gestione del software sono molti: può mettere in una posizione migliore durante la trattativa con fornitori di software e garantire il possesso delle informazioni necessarie per essere sicuri per quanto riguarda gli accordi di acquisto del software.

**Consente una pianificazione più strategica ed evita i problemi di under e overlicensing, riducendo i costi amministrativi e di supporto dell'IT e i costi associati.**

**Il reparto IT dell'azienda o l'assistenza tecnica possono controllare meglio a quale software hanno accesso i dipendenti e la loro capacità di introdurre software non autorizzato in rete.**

## L'impatto economico

La pirateria del software non ha conseguenze negative soltanto sull'ambiente aziendale, ma ha implicazioni di più ampia portata per l'economia in generale. La pirateria priva i fornitori di software di ricavi che investirebbero nella ricerca, nello sviluppo e in nuovi posti di lavoro. Poiché il software ha un ruolo fondamentale nell'information economy, la pirateria ha un effetto che incide su altri ambiti del settore IT e sull'economia in generale.

Il settore IT non soltanto impiega centinaia di migliaia di persone e contribuisce notevolmente al PIL, ma porta produttività nella maggior parte delle aziende. È quindi fondamentale che le aziende riconoscano il valore del software e si assicurino che ogni programma sia legale e dotato di licenza adeguata.

Best practice e un approccio oculato alla responsabilità sociale d'impresa promuovono fair play e comportamento etico in azienda, oltre alla necessità di rispondere ad azionisti/proprietari. Questo vale anche per le società che sviluppano il software che risulta di così vitale importanza per altre imprese.



## Software senza licenza: quali sono i rischi?

Secondo uno studio commissionato da BSA<sup>3</sup>, un quinto delle PMI europee ritiene che non esista alcun rischio legato all'installazione, al download o all'uso di software senza licenza. Esistono invece molti rischi per l'azienda legati a questa pratica, e supporre che non esista alcun rischio e credere che l'uso di software senza licenza sia qualcosa di cui non ci si debba preoccupare è una tendenza preoccupante. Non comprendere i rischi legati all'uso di software senza licenza può esporre l'azienda a numerosi pericoli.

**Le conseguenze dell'uso di software senza licenza possono incidere su un'azienda da un punto di vista operativo, tecnico, finanziario e legale.**



<sup>3</sup> Fonte: ricerca sul rischio commerciale "Commercial Risk" condotta da GfK NOP, 2007

## Rischi operativi e tecnici

### Perdita e danneggiamento di dati

Dagli studi condotti da IDC<sup>4</sup> è emerso che il software pirata, ottenuto tramite download illegali o CD contraffatti, ha una possibilità su due di contenere "codice aggiuntivo", come Trojan, virus o spyware, che può causare danni ai sistemi IT o rivelare dati aziendali riservati a intrusi. Il software piratato potrebbe inoltre non garantire l'applicazione di patch di protezione. In alcuni casi è possibile applicare al software senza licenza soltanto patch considerate critiche. Tempo di inattività e violazioni della sicurezza potrebbero avere immediati effetti negativi sui profitti.

### Perdita di funzionalità

Oltre ai rischi di sicurezza legati all'uso di software piratato scaricato da siti Web o reti P2P, tale software è spesso al di sotto degli standard, oppure potrebbero verificarsi una perdita di funzionalità e problemi di compatibilità che non si avrebbero con le versioni legali con licenza. Le copie senza licenza potrebbero non ricevere tutti gli aggiornamenti dai fornitori. Di conseguenza, i dipendenti non possono utilizzare il software completo, dando ai concorrenti un vantaggio in quanto essi possono rispondere in modo più veloce, completo ed efficace grazie al possesso degli strumenti necessari. Esiste inoltre il rischio che i dati vengano danneggiati o non vengano salvati correttamente, con la conseguente perdita di dati importanti.

### Assenza di assistenza tecnica

Dato che le attività aziendali dipendono così tanto dall'IT, è essenziale la presenza di adeguati sistemi di assistenza. Gli utenti di software senza licenza spesso non hanno accesso alla fondamentale assistenza tecnica offerta dai fornitori e di conseguenza operano in modo meno efficiente.

### Danno alla reputazione

Anche se è difficile da quantificare, il danno innegabile alla reputazione di un'azienda che viene scoperta a utilizzare software illegale è un rischio reale: basta pensare alle conseguenze che si potrebbero avere se i propri clienti non ricevessero il livello di assistenza che si aspettano. In effetti, un sondaggio effettuato nel Regno Unito ha rivelato che il 42% delle persone ritiene che se i loro clienti venissero a conoscenza del fatto che usano software illegale, sarebbero meno propensi a fare affari con loro<sup>5</sup>.

<sup>4</sup>Fonte: studio "The Risks of Obtaining and Using Pirated Software" condotto da IDC, 2006

<sup>5</sup>Fonte: ricerca sull'etica aziendale "Corporate Ethics" condotta da YouGov, 2006

## Rischi finanziari e legali

### Sanzioni legali

Lo sviluppo di software richiede anni di investimento. Unisce le idee creative e il talento di programmatori, sviluppatori e grafici. Come la maggior parte dei lavori creativi, il software informatico è protetto dalle leggi sul copyright, che devono essere rispettate dagli utenti affinché il settore del software possa continuare a innovarsi.

Quando si acquista un software, non si acquista anche la proprietà del copyright. Acquistando una licenza si diventa licenziatario del copyright: si ha cioè il diritto di utilizzare il software a determinate condizioni imposte dal detentore del copyright, che generalmente è il produttore del software. La licenza è un documento legale che definisce le condizioni di utilizzo di qualsiasi prodotto software. Se un'azienda viola le condizioni di una licenza software, per esempio copiando, distribuendo o installando volontariamente o meno il software in modi vietati dalla licenza, infrange il copyright e la legge. Le sanzioni civili e penali variano a seconda del Paese europeo, ma si potrebbero ricevere multe salate.

### I costi dell'essere scoperti

Se si è sospettati di utilizzo di software senza licenza, Business Software Alliance prenderà provvedimenti. Se si viene giudicati colpevoli di violazione della legge sul copyright del software per avere installato software senza licenza sui PC aziendali, l'azienda dovrà pagare ingenti danni e sostenere elevati costi legali. Dovrà inoltre acquistare le versioni legali del software necessarie per continuare l'attività.

### Multe

A seconda del settore in cui si opera, l'uso di software senza licenza potrebbe comportare il pagamento di multe emesse da vari organismi come enti finanziari, forze dell'ordine ed enti per la tutela dei dati. Molti di questi enti hanno dei criteri che determinano le procedure ammissibili e il possesso di software senza licenza potrebbe influire su tali procedure, esponendo l'azienda a ulteriori sanzioni finanziarie.

### Costi di risoluzione del problema

Se scoperte in possesso di software illegale, le aziende spesso sono obbligate a eliminare tutte le versioni senza licenza, dovendole quindi sostituire con le versioni legali. Non vale proprio la pena assumersi questo tipo di rischio prendendo scorciatoie quando si tratta di licenze software, per non parlare dei disagi che potrebbero essere arrecati all'azienda da una causa legale.

## Come finisce il software senza licenza sui PC dell'azienda?

Il software senza licenza nell'azienda potrebbe provenire da varie fonti: download non autorizzati da parte di dipendenti, download nascosti tramite finestre a comparsa visualizzate durante la visita di alcuni siti Web e inadeguata gestione delle licenze software sono soltanto alcune di queste. Le cause di tali errori sono spesso la mancanza di consapevolezza tra i dirigenti aziendali e i dipendenti, politiche IT inadeguate e inefficaci processi di gestione del software. Purtroppo in alcuni casi l'uso di software senza licenza è volontario e la direzione è a conoscenza della situazione, ma indubbiamente non dei relativi rischi.

Gli approcci per risolvere i problemi identificati di seguito vengono spiegati nella sezione "Come ridurre i rischi".

### **Inadeguata gestione del software e delle licenze software**

La comprensione dell'importanza del software e la conoscenza dei tipi di software e di licenze disponibili può influire notevolmente sulla modalità operativa dell'azienda e sulla sua espansione, quindi dovrebbe essere presa in considerazione quando si prendono decisioni aziendali. Migliorando la conoscenza delle risorse software della propria azienda e verificando che vengano gestite e protette nel modo migliore, possono essere utilizzate in modo più efficace per aumentare produttività ed efficienza.

Sono a disposizione vari tipi di licenze software per soddisfare le diverse esigenze: da semplici formati "di accettazione con un clic" ad accordi molto più complessi. La flessibilità aumenta di anno in anno. Molte licenze standard consentono l'installazione su un numero di PC che varia da uno a cinque, mentre i contratti di licenza a volume consentono solitamente un numero fisso di installazioni da effettuare con l'ausilio di un CD master. Qualsiasi installazione eccedente i livelli concordati deve essere autorizzata dal produttore o rivenditore del software. Troppo spesso la mancanza di un'accurata documentazione da parte dell'azienda delle installazioni effettuate o di rigide politiche aziendali può portare le aziende a violare la legge.

L'underlicensing si verifica quando il software viene installato su un numero di PC maggiore di quello consentito dalla licenza, ed è una conseguenza comune di una gestione di software e licenze software inefficace. Se la licenza consente l'installazione del software su venti computer desktop, il software installato su ulteriori computer desktop è senza licenza e viola quindi le condizioni della licenza. Di fatto si tratta di una copia illegale ed essere scoperti con software senza licenza comporta notevoli rischi, come indicato in precedenza.

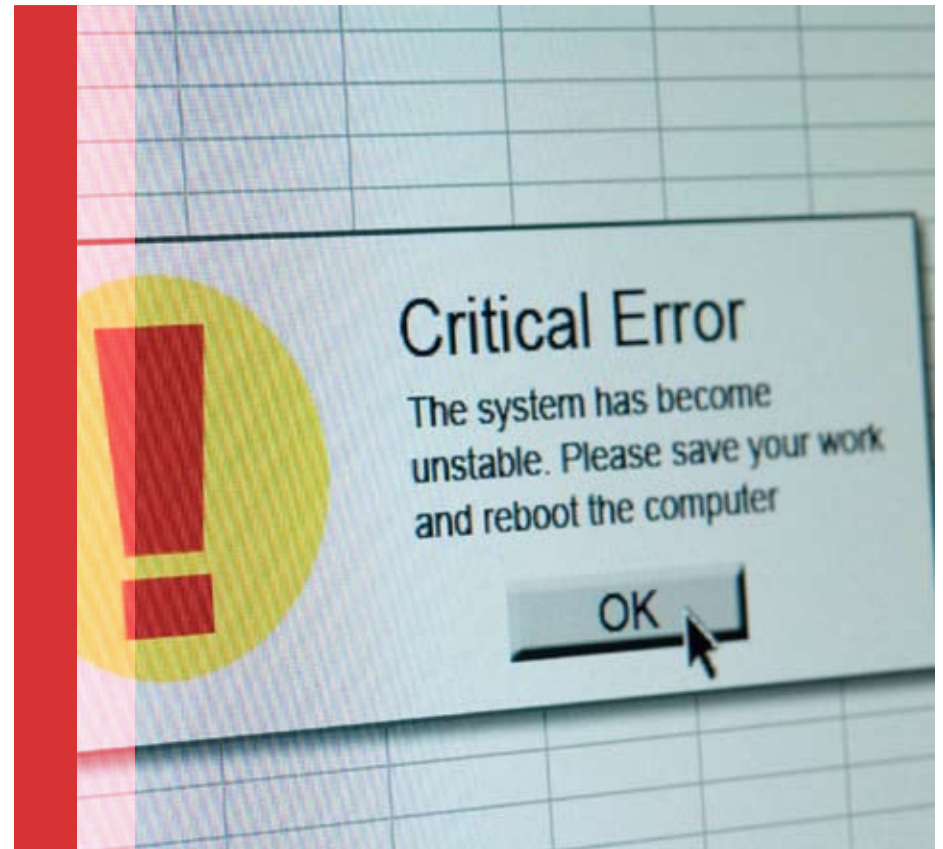
## Download da Internet

Internet è un prezioso strumento aziendale molto utilizzato da numerose aziende, che però dà anche la possibilità di scaricare software non approvato dall'azienda e non autorizzato sui PC aziendali, a meno che vengano effettuati adeguati controlli.

Poiché l'accesso a Internet è diventato più veloce, è molto più semplice acquistare e/o scaricare musica, film e altri elementi multimediali. Diventa sempre più facile spostare prodotti da un computer all'altro senza alcun supporto fisico e con il minimo rischio di essere scoperti. La pirateria che un tempo richiedeva la conoscenza di complessi codici informatici ora è possibile con un clic del mouse.

Senza una tecnologia di blocco che impedisca tali download non autorizzati, i dipendenti possono scaricare software senza che i dirigenti lo sappiano o abbiano dato il consenso.

Esiste una serie di rischi legati a questa attività. Se un dipendente ha installato software senza licenza, il proprietario o l'amministratore delegato dell'azienda è comunque responsabile della violazione del copyright e l'azienda potrebbe dover affrontare rischi legali e finanziari. Se l'origine del software non è nota, il software scaricato potrebbe contenere virus, spyware o Trojan a cui verrebbe dato accesso diretto alla rete IT aziendale.



Esiste anche un rischio sempre maggiore legato alle “finestre a comparsa” che appaiono sullo schermo quando vengono visitati certi siti Web, spesso quelli che offrono software “in offerta speciale” o immagini da scaricare. A volte questi siti sono solo una copertura per attività illegali e installano software, virus o spyware sul PC convincendo il dipendente a fare clic nella finestra con l’inganno.

### **Siti di aste su Internet**

Uno dei maggiori successi di Internet è senza dubbio costituito dai siti di aste. È possibile vendere libri, giocattoli, pezzi da collezione e persino case online. La flessibilità, la velocità e il successo di questi siti è prova non soltanto della loro popolarità, ma anche dei vantaggi che offrono ad acquirenti e venditori. Tuttavia, tra le tante offerte oneste e autentiche si nascondono trappole per acquirenti incauti. I prezzi più economici di software apparentemente originali possono essere allettanti per le piccole aziende in espansione che desiderano ridurre i costi. Tuttavia, la possibilità di celare l’identità o di creare false identità ha portato molte persone a utilizzare questo mezzo per svolgere attività illegali, e i siti di aste sono diventati il veicolo preferito per chi cerca di vendere software senza licenza o piratato.

### **Da uno studio condotto nel 2006 da IDC è emerso che meno del 49% dei software Microsoft offerti su eBay era originale.<sup>6</sup>**

Quando si capisce di avere acquistato software illegale può essere molto complicato ottenere un risarcimento. Tra i clienti “imbrogliati” che hanno presentato reclami, pochissimi hanno ottenuto un rimborso per i loro acquisti. Inoltre, alcuni di coloro che hanno avuto indietro il denaro, generalmente dopo aver dedicato molto tempo e fatica alle richieste di risarcimento, hanno spesso ricevuto somme inferiori al costo degli articoli piratati.

<sup>6</sup> Fonte: studio “The Risks of Obtaining and Using Pirated Software” condotto da IDC, 2006

## Lavoro mobile

La forza lavoro di tutto il mondo sta diventando sempre più mobile grazie a datori di lavoro che forniscono al loro staff una serie di dispositivi per lavorare in modo più efficiente a casa o fuori ufficio.

Tuttavia, questa maggiore libertà comporta nuovi problemi:

la diffusione di dispositivi utilizzati fuori ufficio e a casa ha aumentato le possibilità per lo staff di scaricare software illegale sulle reti dei datori di lavoro. L'azienda è responsabile anche dei software installati sui portatili perché sono comunque una risorsa aziendale. Lo stesso vale per i PC che i dipendenti possono utilizzare a casa ma che sono di proprietà del datore di lavoro.

Le eventuali norme di utilizzo di Internet devono quindi includere norme relative all'utilizzo delle risorse aziendali presso l'abitazione dei dipendenti.

## Fornitori "fasulli"

Esiste una minoranza di fornitori di software che infrange le regole e vende consapevolmente merci illegali.

Molte PMI affidano la gestione dell'IT a fornitori esterni, quindi è fondamentale verificare con cura le credenziali del proprio fornitore di software.

Occorre accertarsi che il proprio fornitore o rivenditore di software sia in grado di dimostrare il fatto che reperisce il software da canali di distribuzione autorizzati.

**È possibile verificare facilmente i metodi di distribuzione autorizzati contattando direttamente i produttori di software e domandando loro chi sono i fornitori autorizzati a distribuire i loro prodotti.**

## Come ridurre i rischi

Esiste una serie di passaggi che l'azienda può svolgere per ridurre al minimo i rischi legati al software senza licenza.

### Controlli regolari e politiche di utilizzo efficaci

Non si tratta di un "problema tecnologico" ma aziendale, che spesso può essere risolto implementando delle best practice. Considerati i rischi, ottenere il supporto a livello aziendale per attuare determinati processi è fondamentale.

Ogni azienda dovrebbe almeno controllare regolarmente il software installato sui propri PC e attuare delle politiche per i dipendenti relative al corretto utilizzo della tecnologia aziendale (compresa la tecnologia utilizzata a casa o i dispositivi mobili utilizzati dai dipendenti ma di proprietà dell'azienda). Dovrebbe essere chiarito il fatto che le politiche saranno fatte rispettare e, quando possibile, dovrebbero essere coinvolti i responsabili del personale per garantirne l'applicazione.

### Software Asset Management

Stranamente, un terzo delle PMI non ha mai sentito parlare di Software Asset Management.<sup>7</sup>

Software Asset Management (SAM) è una metodologia che aiuta le aziende a definire e implementare dei processi per ottimizzare i loro investimenti in software. Sufficientemente flessibile per le aziende di qualsiasi dimensione e per qualsiasi fase dello sviluppo, un sistema SAM può identificare i punti deboli dell'azienda che la espongono ai rischi trattati in precedenza e garantire l'attuazione di processi per ridurre la probabilità di incorrere in tali rischi o evitarli del tutto.

Il sistema SAM considera in forma integrata dipendenti, processi e, quando necessario, tecnologia per garantire che le risorse software vengano gestite, protette e utilizzate nel modo più efficace ed efficiente possibile. Inoltre, le licenze e il loro utilizzo vengono sistematicamente controllati, valutati e gestiti. I vantaggi del sistema SAM per l'azienda possono essere notevoli: oltre a dare tranquillità, può aiutare a ridurre i costi per l'IT perché le società possono pianificare e stimare in modo preciso le proprie esigenze in termini di software, compresi software di recente acquisizione e gli aggiornamenti delle licenze.

Per implementare un sistema SAM in modo efficace all'interno dell'azienda è possibile svolgere una serie di passaggi. Non occorre mettere in gioco tutti questi elementi dall'inizio (ognuno dei quali porterà dei miglioramenti), ma riconoscere che il software è una risorsa aziendale fondamentale e che la sua gestione è una questione aziendale prioritaria.

<sup>7</sup>Fonte: ricerca sul rischio commerciale "Commercial Risk" condotta da GfK NOP, 2007

## Otto passaggi per implementare un sistema di Software Asset Management:

### 1 **Ottenere il supporto dell'intera azienda**

L'implementazione di un sistema SAM comporta un significativo cambiamento culturale; è fondamentale assicurarsi che sia i dirigenti che gli utenti finali supportino il progetto e riconoscano la necessità del sistema SAM.

### 2 **Nominare un responsabile delle risorse software**

A meno che esista una persona che supervisioni il software dell'intera azienda, è molto complicato tenere sotto controllo le risorse software. Il responsabile non deve essere qualcuno del reparto IT ma, a seconda delle dimensioni dell'azienda, è meglio che sia la persona responsabile della gestione dell'IT, che è quindi coinvolta nell'acquisto di software. Se si dispone soltanto di una persona responsabile dell'IT, come spesso accade nelle aziende più piccole, renderlo esplicito nella descrizione delle sue mansioni.

### 3 **Controllare il software corrente e l'utilizzo delle licenze**

Sarà necessario fare un inventario delle proprie risorse software per sapere esattamente quali software sono in esecuzione nell'azienda e quali licenze sono necessarie per il software.

Solo sapendo quali programmi sono installati, di quanti computer dispone la propria azienda e se sono state installate copie di programmi dai propri dipendenti sarà possibile identificare i potenziali rischi o problemi e prendere provvedimenti per evitarli.

### 4 **Creare un database per la gestione delle risorse software**

Disporre di un valido database in cui archiviare tutte le informazioni relative al proprio software è fondamentale per la riuscita della strategia SAM. È possibile utilizzare un foglio di calcolo o investire in uno strumento ideato ad hoc; si rivelerà prezioso.



5

### **Accentrare l'acquisto e la distribuzione del software**

Se non esiste un'unica figura responsabile degli acquisti di software, sarà quasi impossibile capire tutti i vantaggi del sistema SAM.

6

### **Formulare politiche e procedure**

Il controllo dei modi in cui il software entra in azienda è una delle migliori misure preventive che sia possibile attuare. Una politica chiara e rigorosa per i dipendenti, che stabilisca ciò che è consentito e ciò che non lo è, aiuterà a tenere sotto controllo la situazione.

Se si riesce a garantire che i propri collaboratori comprendano pienamente e supportino le strategie di gestione delle risorse software, si contribuirà a controllare l'ambiente in cui viene introdotto il software all'interno della propria organizzazione.

7

### **Effettuare controlli regolari**

Occorre essere consapevoli che SAM è un processo continuo che richiede controlli regolari perché possa funzionare regolarmente e in modo efficiente.

8

### **Rivolgersi a un consulente imparziale per assistenza**

Per aiutare le aziende che desiderano evitare i rischi legati all'uso di software senza licenza, Business Software Alliance ha creato una risorsa online sul suo sito Web ([www.bsa.org](http://www.bsa.org)), che fornisce consigli e strumenti per la gestione del software. Per ulteriori informazioni, consultare la sezione relativa a strumenti e risorse.



## Che cosa fare se si ritiene di poter essere a rischio?

Le aziende dovrebbero considerare il software come qualsiasi altra risorsa preziosa. Prendendo provvedimenti e seguendo i suggerimenti qui forniti, è possibile gestire i rischi aziendali legati all'uso di software illegale e ottenere i vantaggi di un ambiente IT più efficiente.

Se, però, si teme che la propria azienda sia a rischio a causa di software illegale, ci si può rivolgere a diversi soggetti per ricevere assistenza. Rivenditori e fornitori dovrebbero essere i primi a cui rivolgersi per avere risposta a eventuali domande relative alle licenze software.

Altri strumenti a disposizione sul sito Web di BSA sono:

**1 Guida alla gestione del software e al licensing:**  
Opuscoli che possono essere scaricati in sette lingue che consentono alle aziende di implementare procedure di gestione del software e chiarire la conformità alle licenze.

**2 Elenco di fornitori di strumenti per la gestione delle risorse:**  
Un elenco di collegamenti ai principali fornitori di software e ai consulenti che potranno aiutare le aziende con le licenze e nell'implementazione di programmi di gestione del software.

## Fare un check up gratuito online

Lo strumento Healthcheck è stato ideato da BSA per aiutare le aziende a identificare, conoscere e gestire in modo più efficace le risorse IT. In pochi minuti è in grado di:

1. Eseguire un'analisi della posizione SAM attuale.
2. Evidenziare le aree di potenziale vulnerabilità.
3. Consigliare miglioramenti.
4. Generare un report Healthcheck personalizzato dei dati registrati.

<http://global.bsa.org/healthchecktool>

## Appendice: risultati più significativi della ricerca condotta da Gfk NOP

Nel 2007, BSA ha commissionato uno studio a livello europeo per esaminare gli atteggiamenti delle PMI verso la pirateria del software e verificare se esiste una buona conoscenza dei rischi legati all'uso di software illegale nelle aziende.

**1** Il 94% delle PMI europee afferma che l'IT è "molto" o "piuttosto" importante per la capacità di lavorare con successo.

**2** In Europa (Russia esclusa) un quinto degli intervistati ritiene che non esista "alcun rischio" legato all'uso di software senza licenza.

**3** L'87% non si rende conto che l'uso di software illegale potrebbe rendere più vulnerabili ai virus.

**4** Il 97% non considera un problema dover utilizzare versioni vecchie del software a causa dell'impossibilità di effettuare aggiornamenti da versioni illegali.

**5** Il rischio più comune citato dagli intervistati è rappresentato dai "procedimenti penali" (23%), seguito da "sanzioni finanziarie" (21%). Soltanto il 3% ha dichiarato che "dover utilizzare vecchie versioni e non poter effettuare aggiornamenti" è un rischio, nonostante la minaccia commerciale rappresentata dai concorrenti che usano le soluzioni più aggiornate.

**6** Tuttavia, le PMI dell'Europa centrale e orientale e della Russia che considerano "perdita e danneggiamento di dati" un rischio dell'uso di software senza licenza sono il doppio rispetto alle aziende dell'Europa occidentale. In Russia, gli "errori del software" erano considerati un rischio dal 27%, mentre soltanto l'8% delle aziende occidentali condivideva questa opinione.

**7** È più probabile trovare dei processi per la gestione dell'uso di software nelle PMI più grandi con 100 - 250 dipendenti (37%) che in quelle più piccole (19%).

**8** Nel complesso, i "controlli regolari dei PC dei dipendenti" rappresentano il metodo preferito di controllo e gestione dell'uso del software (33%), seguito dalla "politica aziendale" (25%).

## La ricerca

La ricerca è stata condotta per conto di BSA da Gfk NOP tramite sondaggi telefonici su 1.800 aziende di piccole e medie dimensioni europee operanti in Regno Unito, Francia, Germania, Olanda, Italia, Spagna, Russia, Polonia e Ungheria.

Sono state effettuate 200 interviste in ogni Paese. Per gli scopi di questa ricerca, sono state considerate PMI le aziende con un minimo di 10 e un massimo di 250 dipendenti.



#### **BSA Worldwide Headquarters**

1150 18th Street, NW  
Suite 700  
Washington, DC 20036  
USA  
Telefono: +1 202 872 5500  
Fax: +1 202 872 5501

#### **BSA Europa, Medio Oriente, Africa (EMEA)**

2 Queen Anne's Gate Buildings  
Dartmouth Street  
London SW1H 9BP  
United Kingdom  
Telefono: + 44 (0) 20 7340 6080  
Fax: + 44 (0) 20 7340 6090

#### **BSA Asia-Pacifico**

300 Beach Road  
#25-08 The Concourse  
Singapore 199555  
Telefono: + 65 6292 2072  
Fax: + 65 6292 636

<http://www.bsa.org>

Business Software Alliance (BSA) è portavoce dei settori software, hardware e Internet presso gli enti governativi e i consumatori finali nei mercati internazionali. I membri di BSA rappresentano le industrie con il massimo indice di espansione al mondo. BSA svolge attività di informazione e sensibilizzazione sul tema del diritto d'autore, del software e della sicurezza informatica; sostiene politiche che promuovono l'innovazione e incrementano le opportunità di business, combatte la pirateria del software.

BSA, Business Software Alliance e il logo BSA sono marchi di Business Software Alliance Incorporated e potrebbero essere registrati in alcune giurisdizioni.

© 2007 Business Software Alliance. Tutti i diritti riservati.