Considerazioni essenziali per la protezione dei dati sensibili mediante strumenti di prevenzione della perdita di dati

Nageswaran Kumaresan, Ph.D., CISA, CRISC, CGMA, CIA, è uno dei principali responsabili dell'auditing IT presso l'azienda General Motors (GM) e vanta una notevole esperienza nella gestione di numerosi auditing di alto profilo a livello globale all'interno di GM, tra cui sulla implementazione di sistemi per la prevenzione della perdita di dati e sulla attuazione delle policy aziendali. In precedenza ha lavorato per IBM Consulting, PricewaterhouseCoopers e Deutsche Bank.

La protezione delle risorse digitali e della proprietà intellettuale (PI) è un impegno sempre più gravoso per le organizzazioni. Il continuo incombere di liti in materia di brevetti e le battaglie legali per rivendicare la proprietà intellettuale dimostrano l'importanza della tutela della PI al fine di ottenere un vantaggio competitivo. Secondo le stime indicate in un rapporto dell'Ufficio Statunitense Brevetti e Marchi, pubblicato nel 2010, i settori ad alto contenuto di PI degli Stati Uniti generano 5,06 trilioni di dollari in valore aggiunto, ovvero il 34,8% del prodotto interno lordo (PIL) degli Stati Uniti.[1] Inoltre le organizzazioni gestiscono dati personali, finanziari e aziendali sensibili, talvolta disciplinati da leggi e regolamenti di giurisdizioni sia locali che internazionali. Le organizzazioni sono tenute ad adottare misure adeguate per prevenire la perdita e la fuga di dati.

Da studi recenti è emerso che la causa principale della perdita di dati nel mondo aziendale è l'intrusione informatica dall'esterno;[2, 3] tuttavia le organizzazioni dispongono di scarsi meccanismi per valutare e segnalare le perdite di dati che si verificano internamente. Le architetture tecnologiche avanzate, quali firewall, sistemi di rilevamento delle intrusioni, analisi della vulnerabilità e penetration testing, sono progettate principalmente per proteggere la rete dalle minacce esterne. Il controllo della perdita o della fuga di dati internamente richiede architetture diverse, incentrate sulla gestione dei dati all'interno dell'organizzazione e sul flusso di dati verso l'esterno. Ogni giorno una grande quantità di dati digitali fuoriesce dalle reti delle organizzazioni in forma di e-mail, upload di dati, trasferimenti di file e messaggi istantanei. La perdita interna di dati può essere dovuta ad attività illecite, quali sabotaggio informatico, furto di PI e dati sensibili o frode, perpetrate da persone appartenenti all'organizzazione, oltre che a negligenza o ad errore umano.[4] Gran parte delle perdite di dati all'interno delle aziende è dovuta più alla negligenza degli utenti che ad intenzioni dolose.[5, 6] La perdita di dati accidentale o dovuta alla negligenza degli utenti interni è da imputare alla scarsa comprensione delle procedure di gestione dei dati, alla mancanza di *policy* e linee guida efficaci e all'errore umano.[7] Le soluzioni tecnologiche per la prevenzione della perdita di dati (*Data Loss Prevention*, o DLP) riguardano le perdite accidentali o dolose, provocate soprattutto da utenti interni, e definiscono *policy* all'interno del sistema volte a prevenire o a rilevare la fuoriuscita di dati sensibili.

Dal 2006/2007[8] le soluzioni tecnologiche DLP si sono evolute in modo da offrire un approccio aziendale integrato volto a prevenire, rilevare e combattere la diffusione non autorizzata di dati sensibili attraverso la rete di un'organizzazione. La tecnologia DLP viene considerata come uno dei 20 principali requisiti di controllo per garantire la sicurezza delle organizzazioni.[9] Tuttavia, da indagini recenti emerge che l'adozione e l'uso della tecnologia DLP nel mercato sono scarsi e spesso inefficaci.[10] Le indagini svolte hanno rivelato inoltre che le soluzioni DLP vengono implementate solo in alcuni ambiti, ad esempio per il monitoraggio del web e dell'e-mail, ma non come soluzioni integrate.[11]

Ad alcuni problemi comuni non viene prestata sufficiente attenzione durante l'implementazione delle soluzioni DLP. Di seguito sono descritte dieci considerazioni essenziali che potrebbero aiutare le organizzazioni a pianificare, implementare, applicare e gestire le soluzioni DLP, aggiungendo valore all'organizzazione stessa.

SOLUZIONI DLP: COME FUNZIONANO

Le soluzioni DLP utilizzano le tecnologie di analisi dei contenuti e di DCI (*Deep Content Inspection*) per determinare la riservatezza dei contenuti e prevenire o impedire l'uscita dei dati sensibili dalla rete dell'organizzazione. Le soluzioni DLP integrate supportano inoltre la crittografia di dati e supporti, la raccolta di dati correlati a malware, il monitoraggio dell'accesso agli archivi di dati sensibili, l'individuazione e la classificazione di dati. La definizione e l'implementazione di *policy* DLP appropriate consentono di monitorare endpoint specifici, archivi di dati e gateway per il trasferimento di dati, nonché di bloccare determinate attività e spostamenti di dati.

In linea generale, le soluzioni DLP riguardano attività a tre livelli distinti:

- **Livello client (operativo)**—Le *policy* sono definite e implementate in base agli endpoint utilizzati dai dipendenti per lo svolgimento

delle quotidiane mansioni lavorative. Le attività degli utenti che violano le *policy* predefinite vengono monitorate o bloccate dagli agenti DLP installati nei terminali endpoint degli utenti.

- **Livello rete (transito)**—Le *policy* DLP riguardano gli spostamenti di dati al di fuori della rete dell'organizzazione. I dati trasmessi da una posizione a un'altra vengono monitorati e, se necessario, bloccati dal sistema DLP in corrispondenza dei gateway di rete ed e-mail. I pacchetti di dati trasmessi vengono controllati mediante tecniche di *deep content inspection* dei pacchetti, per verificare la natura dei contenuti in transito. Viene inoltre verificata la conformità alle *policy* dei trasferimenti di dati tramite e-mail (SMTP), web (HTTP/HTTPS) e trasferimento di file (FTP/FTPS), al fine di prevenire o intercettare la perdita di dati sensibili.
- **Livello archivio (riposo)**—In questo caso vengono controllati i dati statici archiviati nei server. I dati sensibili memorizzati negli archivi dati vengono analizzati in base a regole specifiche, mediante l'uso di crawler per individuare la posizione e valutare il grado di riservatezza dei dati nonché l'adeguatezza degli archivi in cui sono conservati rispetto alle *policy* aziendali. Vengono utilizzati sistemi di rilevamento automatico (*discovery scan*) per classificare o contrassegnare i file e consentirne il successivo monitoraggio degli accessi.

10 CONSIDERAZIONI ESSENZIALI

Alla luce di quanto appreso attraverso l'esperienza di molteplici precedenti implementazioni DLP, di seguito vengono presentate 10 considerazioni essenziali che potrebbero aiutare le organizzazioni ad implementare con successo una soluzione DLP quale meccanismo di protezione dei dati:

1. **Implementazione di un approccio olistico e individuazione del valore aggiunto apportato dai sistemi DLP basate sulla valutazione del rischio**—Le soluzioni DLP dovrebbero essere considerate come parte di un meccanismo generale di sicurezza delle informazioni e della strategia di protezione dei dati. È importante capire l'architettura di sicurezza esistente e valutare quindi in che modo una soluzione DLP può offrire maggiore protezione. Nell'ambito della suddetta valutazione è necessario tenere conto del tipo di dati che l'organizzazione intende proteggere, dei rischi per la sicurezza in base all'architettura di sicurezza presente e futura, del costo complessivo e del valore aggiunto derivante dall'introduzione di una soluzione DLP. L'analisi obiettiva del rapporto tra costi e benefici, considerati il costo della perdita dei dati, il costo totale di implementazione e gestione nonché i potenziali vantaggi, forniscono indicazioni sul valore aggiunto ottenibile da una soluzione DLP. L'analisi del razionale economico di una soluzione DLP e la decisione di implementare o meno tale soluzione dovrebbero fondarsi sulla valutazione e sull'analisi obiettiva dei rischi, tenendo conto dell'orientamento aziendale presente e futuro.
2. **Coinvolgimento delle persone giuste con il modello di organizzazione giusto**—I team aziendali sono fortemente coinvolti nella prevenzione e nel rilevamento dei flussi di dati sensibili. L'esigenza di stabilire *policy* DLP può manifestarsi in diversi ambiti: a livello aziendale (senior management), di valutazione del rischio (gestione del rischio), in relazione ad eventi recenti riguardanti la sicurezza (gestione di protezione IT, requisiti legali e conformità) e minacce/criticità *ad hoc*. Le *policy* DLP devono soddisfare i requisiti legali e i principi di protezione dei dati. I rappresentanti delle funzioni aziendali principali, quali ricerca e sviluppo, progettazione, finanza, conformità e aspetti legali, possono contribuire alla definizione delle *policy* in base ai rispettivi rischi. Coinvolgere fin dall'inizio le persone giuste, con ruoli e responsabilità precisi, è uno dei fattori chiave del successo. Il team DLP deve essere composto da responsabili della protezione dei dati, da proprietari di dati e da rappresentanti delle divisioni principali, del reparto IT e di varie business unit. I membri del team devono ricevere una formazione adeguata riguardo al sistema DLP, al suo utilizzo e alle limitazioni affinché possano attuarne l'implementazione in modo efficace. Il responsabile del team deve avere una buona conoscenza dei requisiti organizzativi e aziendali, nonché del sistema DLP, e deve essere autorizzato a gestire le questioni riguardanti il sistema DLP.
3. **Individuazione dei dati sensibili e comprensione delle modalità di gestione**—Le tecnologie di protezione dei dati orientate ai contenuti, come la tecnologia DLP, sono fortemente basate sulla corretta classificazione delle informazioni. Le *policy* DLP interessano prevalentemente i documenti sensibili e la gestione degli stessi all'interno di un'organizzazione. L'ottimizzazione delle procedure di gestione dei dati sensibili, dalla creazione fino all'archiviazione e all'eliminazione, mediante criteri e procedure adeguati dovrebbe essere una fase essenziale per l'efficace applicazione del sistema DLP. L'individuazione e la classificazione dei dati sensibili, secondo i criteri e le linee guida dell'organizzazione, sono passaggi importanti ai fini dell'attuazione di una strategia di protezione dei dati completa. La corretta definizione delle *policy* DLP richiede inoltre la comprensione delle modalità di gestione dei dati sensibili, delle eccezioni e degli scenari da evitare o da bloccare. Le *policy* e le

procedure devono fornire ai dipendenti istruzioni chiare sulle pratiche appropriate e inappropriate. Programmi di formazione e consapevolezza possono contribuire al raggiungimento di tale obiettivo.

4. **Implementazione graduale in base ai progressi**—Le soluzioni DLP offrono numerose opzioni di implementazione, così da permettere alle organizzazioni di concentrarsi sui settori ad alto rischio. Il monitoraggio di e-mail, web e unità flash USB è una delle opzioni più largamente utilizzate nelle soluzioni DLP.[12] L'implementazione pilota iniziale dovrebbe essere limitata a una sola regione o divisione. Un approccio graduale, con la definizione dei moduli prioritari e degli endpoint chiave, permette di trarre insegnamento dall'esperienza, prima di effettuare un'implementazione su larga scala. È necessario definire un piano di implementazione, comprendente *milestone* e punti di controllo adeguati per valutare i progressi, incluse le decisioni di procedere o meno. I moduli possono essere implementati dapprima in un piccolo gruppo o settore di destinazione, per consentire il perfezionamento dei criteri e ridurre al minimo l'impatto sulle attività aziendali. Il team di implementazione deve analizzare i risultati iniziali in modo oggettivo, tenendo conto delle possibilità di miglioramento, dei vantaggi e dell'impatto operativo.
5. **Impatto minimo sulle prestazioni del sistema e sulle attività aziendali**—Il sistema DLP raccoglie dati da numerosi endpoint e utilizza una significativa quantità di capacità di banda della rete. Gli agenti installati negli endpoint e nei gateway di rete per il monitoraggio dei pacchetti possono influire sulle prestazioni degli utenti. Criteri definiti in modo inaccurato possono generare numerosi eventi e condizionare le prestazioni degli utenti. Ciò provoca insoddisfazione tra gli utenti ed esercita un impatto negativo sul programma DLP. L'implementazione graduale descritta sopra, unitamente a un attento collaudo dei criteri, contribuisce a ridurre al minimo l'impatto sulle prestazioni e a creare un'esperienza positiva per gli utenti. L'infrastruttura DLP e la capacità di rete devono essere pianificate in modo adeguato, per ridurre al minimo l'impatto sulle attività aziendali. La cauta introduzione delle *policy* in un ambiente di prova aiuta a capire l'efficacia dei criteri e il potenziale impatto sulle attività aziendali prima di effettuare un'implementazione su larga scala. Il monitoraggio e la misurazione periodici degli effetti sulle prestazioni di sistema e sugli utenti consentono di valutare i potenziali impatti negativi derivanti da *policy* DLP non adeguatamente definite.
6. **Definizione di *policy* DLP significative e di processi di gestione dei criteri**—La definizione di *policy* pertinenti e significative è di fondamentale importanza per la strategia DLP. La **figura 1** illustra le normali attività operative DLP di un'organizzazione. I criteri vengono definiti allo scopo di monitorare o bloccare (prevenire) la perdita di dati sensibili attraverso la rete di un'organizzazione. Un processo strutturato per la definizione e l'aggiornamento delle *policy* contribuisce ad assicurare che i criteri definiti siano significativi e pertinenti e che non interferiscano con i criteri esistenti. La modifica delle *policy* deve essere gestita mediante un processo controllato. Inoltre le *policy* DLP devono essere riesaminate periodicamente per venire adattate alle nuove tecnologie, pratiche aziendali e situazioni di rischio. Per garantire un'implementazione efficace è necessario definire un processo di gestione del ciclo di vita delle *policy* (**figura 2**), dalla richiesta alla modifica o eliminazione, nonché coinvolgere le persone giuste. Tale processo dovrebbe comprendere una valida attività di gestione dei cambiamenti, inclusi i cambiamenti di emergenza per far fronte alle minacce *ad hoc* specifiche. Prima di procedere all'implementazione su larga scala, è necessario collaudare i criteri in un ambiente ristretto o di prova per verificare che funzionino nel modo auspicato e che non esercitino un impatto negativo.
7. **Implementazione di validi meccanismi di revisione e analisi degli eventi**—Gli eventi generati dalle violazioni delle *policy* e i log attività che ne risultano (in caso di blocco o monitoraggio) sono output chiave di uno strumento DLP, in grado di fornire informazioni e

Figura 1—Normali attività operative DLP

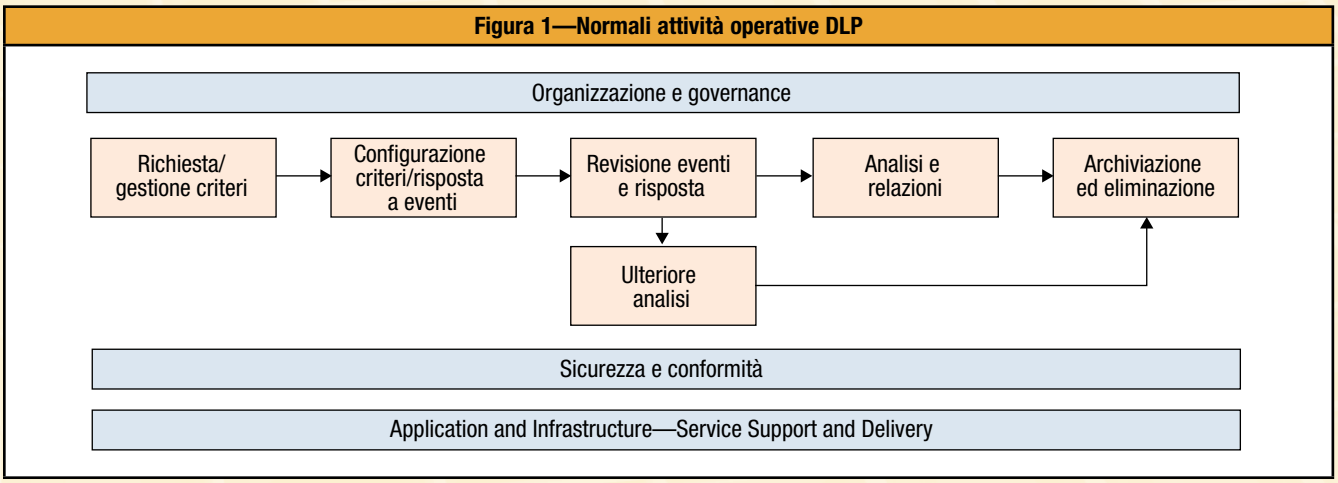
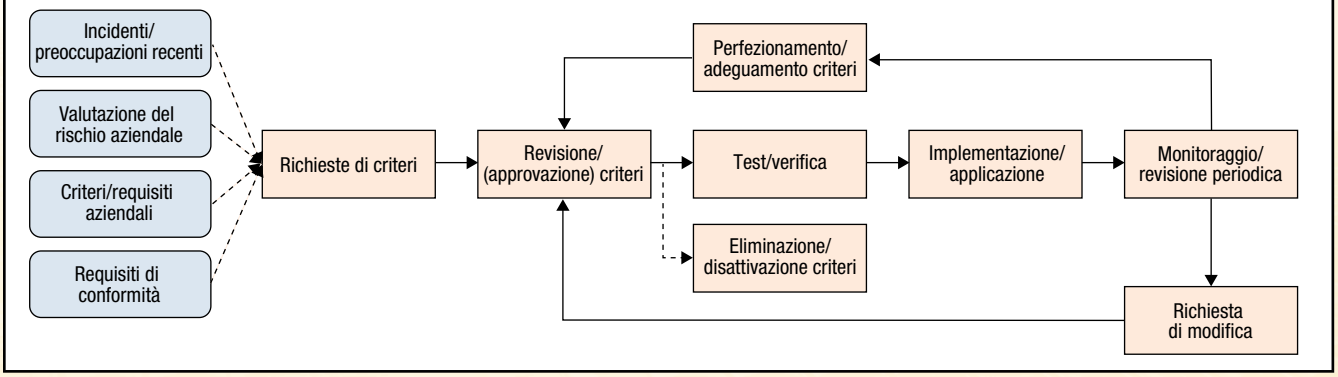


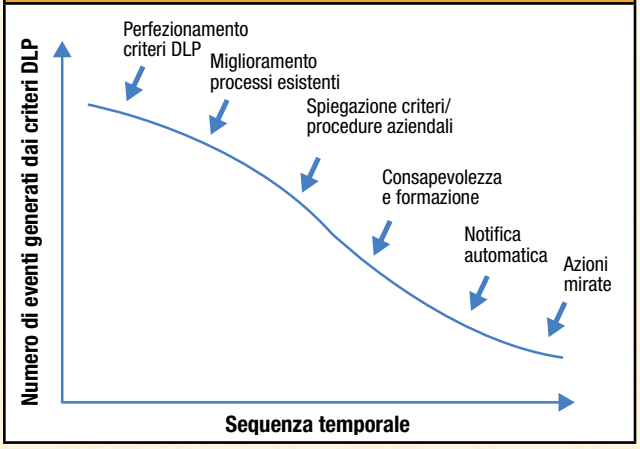
Figura 2—Processo di gestione delle *policy* DLP



conoscenze preziose. Per realizzare i vantaggi offerti dalla soluzione è necessario un meccanismo di revisione efficace e dinamico. Le regole di risposta possono essere definite nel sistema in modo da determinare una risposta specifica caso per caso. Inoltre è possibile configurare allarmi per eventi specifici. Un team di revisione degli eventi rappresentativo e dinamico dovrebbe essere incaricato di esaminare gli eventi critici e di adottare tempestivamente le misure necessarie per prevenire un impatto negativo sulle attività aziendali. Gli incidenti gravi potrebbero richiedere un'analisi approfondita, svolta preferibilmente da un team separato. I dati non più necessari devono essere eliminati per liberare spazio di archiviazione. È necessario stabilire valide regole di risposta agli eventi basate sul rischio per ogni criterio definito, allo scopo di identificare e attribuire la corretta priorità agli eventi insoliti. Il team di revisione degli eventi deve avere una conoscenza adeguata del rischio di business. Il feedback inviato ai referenti di ciascuna *policy* a seguito della revisione degli eventi può fornire informazioni utili per perfezionare i criteri e adottare misure efficaci al fine di ridurre il rumore (falsi positivi) negli eventi generati. La revisione e l'analisi degli eventi devono essere gestite con cautela, attenendosi alle procedure definite per rispettare politiche aziendali, leggi e regolamenti.

8. **Analisi e relazioni significative**—Gli eventi generati dai criteri DLP forniscono informazioni utili su dove, quando e come i dati sensibili vengono archiviati e gestiti all'interno dell'organizzazione. È possibile analizzare gli eventi rispetto a più dimensioni quali ad esempio policy interessate, unità organizzative, aree geografiche, tendenze. Il quadro complessivo può fornire informazioni sulle attuali procedure di gestione dei dati e sugli aspetti per i quali l'organizzazione necessita di maggiore consapevolezza e formazione. Un efficace programma DLP può rafforzare le procedure esistenti che richiedono un miglioramento. Un valido processo di analisi e di informazione mediante relazioni può aiutare i referenti per le diverse *policy* ad aumentare l'efficacia dei criteri DLP. Anche i profili e le tendenze degli eventi possono essere utili per creare o definire meglio i criteri e le linee guida. È opportuno prevedere comunicazioni periodiche mediante relazioni per segnalare modelli e tendenze di perdite di dati alle parti interessate, al fine di migliorare le procedure di controllo e modificare i criteri, se necessario. Lo sviluppo di validi indicatori (metriche) e di un'analisi di modelli e tendenze appropriata, al fine di individuare i cambiamenti e le eccezioni, è uno dei fattori chiave per un'analisi efficiente. In generale, gli eventi di perdita di dati dovrebbero gradualmente diminuire per ciascuna *policy*, se supportati da programmi di consapevolezza e da altre attività di gestione (**figura 3**).
9. **Implementazione di misure di sicurezza e conformità**—Un sistema DLP raccoglie una grande quantità di dati, alcuni dei quali potrebbero essere di carattere personale. La gestione dei dati personali raccolti deve avvenire conformemente alle leggi e ai regolamenti sulla protezione dei dati in vigore nei paesi in cui i dati vengono raccolti. Anche i dati aziendali possono essere sensibili; pertanto è molto importante gestire il sistema DLP e i dati acquisiti in modo sicuro e nel rispetto delle leggi e dei regolamenti applicabili. Al pari di altre tecnologie, anche le soluzioni DLP presentano alcune limitazioni nella prevenzione e nel rilevamento di ogni evento di perdita di dati in un contesto tecnologico dinamico. È quindi necessario comprendere i potenziali scenari ad alto rischio in cui la tecnologia DLP può essere elusa per scopi dolosi e collaborare con i team di sicurezza IT per definire efficienti contromisure di protezione. Al fine di accrescere la sicurezza in generale, è opportuno adottare procedure sicure e controllate per la creazione, l'aggiornamento e l'eliminazione di configurazioni di criteri e la gestione degli eventi all'interno del sistema DLP, nonché stabilire un'appropriata suddivisione dei compiti. È importante conoscere i requisiti di protezione dei dati vigenti in base all'ambito di implementazione e, se necessario, adottare le misure appropriate, come ad esempio la notifica ai dipendenti e l'ottenimento del loro consenso. Il team DLP dovrebbe far parte della struttura di governance della sicurezza aziendale e collaborare strettamente con gli altri team di sicurezza per garantire la protezione dei dati.

Figura 3—Applicazione efficace dei criteri DLP



10. **Implementazione di un flusso di dati organizzativo e di un meccanismo di supervisione**—La condivisione dei dati e i flussi di dati trasversali delle informazioni aziendali rappresentano le linee di comunicazione essenziali di qualsiasi organizzazione innovativa. Ogni giorno, nell'ambito delle normali attività lavorative, le organizzazioni condividono i dati con diversi gruppi, quali fornitori, clienti, partner di ricerca, organismi di regolamentazione e distributori. Oltre a prevenire la perdita e la fuga di dati sensibili, le organizzazioni devono garantire che le soluzioni DLP non ostacolino il corretto flusso di dati all'interno e all'esterno dell'organizzazione. Un team di supervisione dovrebbe esaminare periodicamente i vantaggi offerti all'azienda dal programma DLP e verificarne l'impatto sui flussi di dati regolari all'interno dell'organizzazione. I benefici derivanti da un programma DLP devono essere sottoposti ad una verifica periodica da parte di un team di supervisione. Gli scenari tecnologici in rapida evoluzione possono condizionare l'efficacia della soluzione DLP, che potrebbe non essere in grado di rilevare ogni singola eccezione. Il team di supervisione deve esaminare il costo complessivo e i vantaggi del programma DLP con regolarità. Sulla base delle revisioni periodiche, il team di supervisione può fornire indicazioni in merito all'orientamento strategico del programma DLP.

CONCLUSIONI

Una responsabilità importante della divisione IT consiste nell'accertare che l'organizzazione adotti misure adeguate per prevenire la perdita e la fuga delle informazioni. Spetta al management garantire alle parti interessate l'attuazione di misure adeguate per proteggere le risorse digitali sensibili dell'azienda, inclusi la proprietà intellettuale e i dati personali e finanziari. Una soluzione DLP completa e integrata può fornire controlli ragionevoli volti a prevenire la perdita di dati in ambito interno. Al contempo, implementare efficacemente una soluzione DLP su larga scala richiede una pianificazione accurata, un approccio sistematico e processi efficaci. Le 10 considerazioni essenziali sopra descritte illustrano, per gradi, gli aspetti che possono contribuire al successo di una soluzione DLP creando valore per un'organizzazione. La valutazione delle suddette considerazioni, sebbene non tutte siano applicabili ad ogni organizzazione, può contribuire al successo dell'implementazione di una soluzione DLP e al rispetto delle *policy* aziendali.

NOTE FINALI

[1] US Patent and Trademark Office, "Intellectual Property and the U.S. Economy: Industries in Focus," Economics and Statistics Administration, Marzo 2012, *www.uspto.gov/news/publications/IP_Report_March_2012.pdf*

[2] KPMG, "Data Loss Barometer: A Global Insight Into Lost and Stolen Information," 2012, *www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/data-loss-barometer.pdf*

[3] Verizon, "Data Breach Investigations Report," 2012, *www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf*

[4] Janes, Paul; "Information Assurance and Security Integrative Project: People, Process, and Technologies Impact on Information Data Loss," SANS Institute, 7 novembre 2012, *www.sans.org/reading_room/whitepapers/dlp/people-process-technologies-impact-information-data-loss_34032*

[5] *Op. cit.*, KPMG

[6] ISACA, *Data Leak Prevention*, white paper, Settembre 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Leak-Prevention.aspx*

[7] CSIS, "20 Critical Security Controls, Version 4.1," SANS Institute *www.sans.org/critical-security-controls/guidelines.php*

[8] Kanagasingham, Prathaben; "Data Loss Prevention," SANS Institute, 2008, *www.sans.org/reading_room/whitepapers/dlp/data-loss-prevention_32883*

[9] *Op. cit.*, CSIS

[10] Forrester, "Rethinking DLP: Introducing the Forrester DLP Maturity Grid," September 2012, *www.forrester.com/Rethinking+DLP+Introducing+The+Forrester+DLP+Maturity+Grid/fulltext/-/E-RES61231*

[11] Ashford, Warwick; "Why Has DLP Never Taken Off?," *ComputerWeekly*, 22 gennaio 2013, *www.computerweekly.com/news/2240176414/Why-has-DLP-never-taken-off*

[12] *Op. cit.*, Janes