ISACA®

Trust in, and value from, information systems

Data Leak Prevention

Abstract
Data leak prevention (DLP) is a suite of technologies aimed at stemming the loss of sensitive information that occurs in enterprises across the globe. By focusing on the location, classification and monitoring of information at rest, in use and in motion, this solution can go far in helping an enterprise get a handle on what information it has, and in stopping the numerous leaks of information that occur each day. DLP is not a plug-and-play solution. The successful implementation of this technology requires significant preparation and diligent ongoing maintenance. Enterprises seeking to integrate and implement DLP should be prepared for a significant effort that, if done correctly, can greatly reduce risk to the organization. Those implementing the solution must take a strategic approach that addresses risks, impacts and mitigation steps, along with appropriate governance and assurance measures.

ISACA®

With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA has designed and created *Data Leak Prevention* (the "Work"), primarily as an educational resource for security, governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security, governance and assurance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

Data Leak Prevention

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

ISACA wishes to recognize:

ISACA and IT Governance Institute (ITGI) Affiliates and Sponsors
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants Inc.
ISACA chapters
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
University of Antwerp Management School
Analytix Holdings Pty. Ltd.
BWise B.V.
Hewlett-Packard
IBM
Project Rx Inc.
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

Introduction

Over the last decade, enterprises have become increasingly reliant on digital information to meet business objectives. On any given business day, significant amounts of information fuel business processes that involve parties both inside and outside of enterprise network boundaries. There are many paths for these data to travel and they can travel in many forms—e-mail messages, word processing documents, spreadsheets, database flat files and instant messaging are a few examples. Much of this information is innocuous, but in many cases a significant subset is categorized as "sensitive" or "proprietary," indicating that this information needs to be protected from unauthorized access or exposure. This need can be externally driven by privacy and other types of regulation, or internally driven by business objectives to protect financial, strategic or other types of competitive information.

Most enterprisess employ safeguards to control sensitive information. Often, however, these controls are inconsistent and are managed at different points in the enterprise with different levels of diligence and effectiveness. The result is that despite their efforts, enterprises around the globe leak significant amounts of sensitive information. These leaks create significant risk to enterprises, their customers and business partners with the potential to negatively impact an enterprise's reputation, compliance, competitive advantage, finances, customer trust and business partnerships.

In a study released by IT research company TheInfoPro, DLP was listed as a top priority for enterprise security budgets.

Concerns over this need to better control and protect sensitive information have given rise to a new set of solutions aimed at increasing an enterprise's ability to protect its information assets. These solutions vary in their capabilities and methodologies, but collectively they have been placed in a category known as data leak prevention (DLP). While still an adolescent technology, DLP is seeing an increase in adoption and an increasing number of products entering the market. In a study released earlier this year by IT research company TheInfoPro, DLP was listed as a top priority for enterprise security budgets.[1]

This white paper provides an overview of DLP and explores the benefits, risks and reasons for an enterprise's use of DLP. It also discusses important factors to consider when selecting and deploying a DLP solution. Finally, the paper examines assurance and governance considerations involved in implementing a DLP solution.

It is important to note that while DLP solutions have the ability to intercept some malicious or criminal attempts to steal information, the technology is not yet sufficiently developed to deter more sophisticated methods of data theft. Fortunately, the general consensus is that these cases are a much smaller portion of overall data leak risk. In a report released in March, 2009, the Poneman Institute estimated that 88 percent of data leak incidents were due to user negligence, and 12 percent was due to malicious intent.[2] This low percentage can be somewhat misleading, however, since typically a much greater percentage of malicious data theft will result in adverse actions than with accidental loss.

Defining Data Leak Prevention

Most DLP solutions include a suite of technologies that facilitates three key objectives:
• Locate and catalog sensitive information stored throughout the enterprise
• Monitor and control the movement of sensitive information across enterprise networks
• Monitor and control the movement of sensitive information on end-user systems

---

[1] *SC Magazine*; "Security Spending, DLP Projects to Increase," *www.scmagazineus.com/security-spending-dlp-projects-to-increase/article/164337/*
[2] Trend Micro; *Data-stealing Malware on the Rise—Solutions to Keep Businesses and Consumers Safe, Focus Report Series*, June 2009, USA, *http://us.trendmicro.com/ imperia/md/content/us/pdf/threats/securitylibrary/data_stealing_malware_focus_report_-_june_2009.pdf*

These objectives are associated with three primary "states" of information: **data at rest, data in motion, and data in use**. Each of these three states of data is addressed by a specific set of technologies provided by DLP solutions:

• **Data at rest**—A basic function of DLP solutions is the ability to identify and log where specific types of information are stored throughout the enterprise. This means that the DLP solution must have the ability to seek out and identify specific file types—such as spreadsheets and word processing documents—whether they are on file servers, storage area networks (SANs) or even end-point systems. Once found, the DLP solution must be able to open these files and scan their content to determine whether specific pieces of information are present, such as credit card or social security numbers. To accomplish these tasks, most DLP systems utilize **crawlers**, which are applications that are deployed remotely to log onto each end system and "crawl" through data stores, searching for and logging the location of specific information sets based on a set of rules that have been entered into the DLP management console. Collecting this information is a valuable step in allowing the enterprise to determine where its key information is located, whether its location is permitted within existing policies, and what paths these data might travel that would violate information policies.

• **Data in motion (network)**—To monitor data movement on enterprise networks, DLP solutions use specific network appliances or embedded technology[3] to selectively capture and analyze network traffic. When files are sent across a network they are typically broken into packets. To inspect the information being sent across the network the DLP solution must be able to: passively monitor the network traffic, recognize the correct data streams to capture, assemble the collected packets, reconstruct the files carried in the data stream, and then perform the same analysis that is done on the data at rest to determine whether any portion of the file contents is restricted by its rule set. At the core of this ability is a process known as **deep packet inspection (DPI)**, which enables the DLP data-in-motion component to accomplish these tasks. DPI goes beyond the basic header information of a packet (which is similar to the "to" and "from" information found on a postal envelope) to read the contents within the packet's payload (akin to the letter within the postal envelope). This technology has evolved over the years and is still imperfect, although increases in processing power and new forms of packet identification have greatly aided the development of this technology. This DPI capability allows the DLP system to inspect data in transit and determine contents, source and destination. If sensitive data are detected flowing to an unauthorized destination, the DLP solution has the capability to alert and optionally block the data flows in real or near real time, again based on the rule set defined within its central management component. Based on the rule set, the solution may also quarantine or encrypt the data in question. An important consideration for network DLP is that the data must be decrypted before the DLP solution can inspect the data. Either the DLP solution must have the capability to do this itself (by having this feature and the necessary encryption keys) or there must be a device that will decrypt the traffic prior to its inspection by the DLP module, and re-encrypt once the data have been inspected and allowed to pass.

• **Data in use (end-point)**—Data in use is perhaps the most challenging aspect of DLP. Data in use primarily refers to monitoring data movement stemming from actions taken by end users on their workstations, whether that would entail copying data to a thumb drive, sending information to a printer, or even cutting and pasting between applications. DLP solutions typically accomplish this through the use of a software program known as an agent, which is ideally controlled by the same central management capabilities of the overall DLP solution. Implementing rule sets on an end-user system has inherent limitations, the most significant being that the end-user system must be able to process the rule sets applied. Depending on the number and complexity of the rules being enforced, it may be necessary to implement only a portion of the entire rule set, which can leave significant gaps in the overall solution.

To be considered a full DLP solution, the capability to address the three states of information must exist and be integrated by a centralized management function. The range of services available in the management console varies between products but many, if not most, have the following functions in common:

• **Policy creation and management**—Policies (rule sets) dictate the actions taken by the various DLP components. Most DLP solutions come with preconfigured policies (rules) that map to common regulations, such as two US acts: the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). It is just as important to be able to customize these policies or build completely custom policies.

---

[3] Some DLP capabilities are being embedded into network systems, such as firewalls and e-mail servers, as opposed to serving as dedicated appliances.

- **Directory services integration**—Integration with directory services allows the DLP console to map a network address to a named end user.
- **Workflow management**—Most full DLP solutions provide the capacity to configure incident handling, allowing the central management system to route specific incidents to the appropriate parties based on violation type, severity, user and other such criteria.
- **Backup and restore**—Backup and restore features allow for preservation of policies and other configuration settings.
- **Reporting**—A reporting function may be internal or may leverage external reporting tools.

DLP Program Approach

Implementation of a DLP solution is a complex undertaking that requires significant preparatory activities.

Implementation of a DLP solution is a complex undertaking that requires significant preparatory activities such as policy development, business process analysis, and detailed inventories and analysis of the types of information used by the enterprise. These activities require the involvement of a broad base of stakeholders from both IT and the business units it supports. The following sections outline key considerations for each stage of the implementation process.

Organizational Data Classification, Location and Pathways

Enterprises are often unaware of all of the types and locations of information they possess. It is important, prior to purchasing a DLP solution, to identify and classify sensitive data types and their flow from system to system and to users. This process should yield a data taxonomy, or classification system, that will be leveraged by various DLP modules as they scan for and take action on information that falls into the various classifications within the taxonomy. Analysis of critical business processes should yield the required information. Classifications can include categories such as private customer or employee data, financial data, and intellectual property. Once the data have been identified and classified appropriately, further analysis of processes should facilitate the location of primary data stores and key data pathways. Frequently multiple copies and variations of the same data are scattered across the enterprise on servers, individual workstations, tape and other media. Copies are frequently made to facilitate application testing without first cleansing the data of sensitive content. Having a good idea of the data classifications and location of the primary data stores proves helpful in both the selection and placement of the DLP solution. Once the DLP solution is in place it can assist in locating additional data locations and pathways.

It is also important to understand the enterprise's data life cycle. Understanding the life cycle from point of origin through processing, maintenance, storage and disposal will help uncover further data repositories and transmission paths.

Additional information should be collected by conducting an inventory of all data egress points since not all business processes are documented and not all data movement is a result of an established process. Analysis of firewall and router rule sets can aid these efforts.

Establishing and Socializing High-level Policies and Processes

Once information has been located and classified, policies should be created or modified to define specific classifications and the appropriate handling of each category. Data classification policies should be kept as simple as possible.

Once policies are in place, a high-level workflow plan should be established. This plan should include the data categories that are targeted, the actions that will be taken (and by whom) to address violations, the escalation processes, and any process required for exception requests. Processes should also be established for off-hours and holidays, when key individuals may not be available. It is important that after-hour processes have clear and well-documented procedures, involve individuals who can make appropriate, well-grounded decisions, and that any decisions that are made to provide an after-hours exception are well documented and reviewed by appropriate stakeholders as soon as they are available. There should be a formal exception management process established that documents all pertinent information regarding the exception in question. It is important to also ensure that appropriate incident management processes exist and are functional for each of the categories of rules prior to going live.

> Once information has been located and classified, policies should be created or modified to define specific classifications and the appropriate handling of each category.

Implementation

Enterprises should strongly consider implementing DLP first in a monitoring-only mode. This will allow the system to be tuned and predict the impacts to business processes and the organizational culture. Allowing system-driven alerts to build awareness and to initiate behavioral changes is generally a better approach than to block traffic flows and potentially derail business processes. While leadership may have significant concerns regarding the amount of sensitive data "flying out the door" once the system is activated, initiating actual blocking too soon can cause even greater problems by breaking or severely impeding critical business processes. The hope is that these processes were identified during the preparation stage, but often things are overlooked that quickly come to light when the DLP solution is enabled.

Remediation of Violations

DLP solutions generally provide a great deal of useful information regarding the location and transmission paths of sensitive information. Sometimes, however, this can be a Pandora's Box experience. An enterprise can be quickly dismayed at the volume and extent of its sensitive data footprint and loss, and may be inclined to rush forward to try to address all issues at once, which is a recipe for disaster. It is important that an enterprise be prepared to use a risk-based approach to prioritize and address findings in the most expedient manner possible. All key stakeholders must be involved in this process since it frequently involves allowing one problem to continue temporarily while a larger one is addressed. The analysis and subsequent decisions regarding this process should be well documented and maintained in anticipation of future audits or regulatory inquiries.

Ongoing DLP Program

The DLP solution should be closely monitored and periodic risk, compliance and privacy reports should be provided for appropriate stakeholders (e.g., risk management, compliance management, privacy team and human resources [HR]).

DLP rules should continue to be reviewed and optimized. DLP solutions will not inform administrators that a rule is too broad and could have a significant performance impact on the DLP infrastructure. Enterprises should ensure that all stakeholders are diligent in reporting any new data formats or data types that may not be represented in the existing DLP rule set. A testing and staging environment should be available and used to test the impact of patches and upgrades on the DLP solution. Finally, it is important to continue training and awareness programs, which should be reinforced by the report and alert capabilities of the DLP solution.

Business Benefits of DLP

> As with any set of security controls, the implementation of DLP should support business objectives and provide a tangible benefit to the business.

As with any set of security controls, the implementation of DLP should support business objectives and provide a tangible benefit to the business. The following list highlights some of the most direct benefits of a well-implemented DLP solution:

- **Protect critical business data and intellectual property**—The primary benefit of DLP is the protection of information that is critical for the business. Enterprises maintain many types of information that they must protect for competitive, regulatory and reputational reasons. Information such as customer information, personnel records, health information, undisclosed financial records, product design documents, business plans and proprietary research are a few examples.
- **Improve compliance**—DLP can help an enterprise meet regulatory requirements related to protecting and monitoring data containing private customer and financial information. DLP solutions typically come with preconfigured rules that address data types impacted by significant regulations such as payment card industry (PCI), GLBA and HIPAA. Leveraging these rule sets can simplify efforts to protect data impacted by these regulations.
- **Reduce data breach risk**—By reducing the risk of data leaks, the financial risk to the enterprise decreases. In its 2009 report, the Ponemon Institute estimated the average cost of a data leak in the US at $204 per record.[4] Even with relatively small breaches of records that number in the thousands, each incident potentially represents a significant financial impact.
- **Enhance training and awareness**—While most enterprises have written policies, such policies may be forgotten over time. DLP solutions alert, and at times block, data movement that is in violation of policy and provide an ongoing education to help ensure that users maintain an awareness of policies associated with sensitive data.
- **Improve business processes**—One of the key intangibles of DLP is the development of new policies, controls and testing that help identify broken business processes. Often, the step of simply assessing and cataloging business processes in preparation for a DLP implementation can provide great insights to the enterprise.
- **Optimize disk space and network bandwidth**—An important benefit of DLP solutions is the identification of stagnant files and streaming videos that consume a large amount of IT resources such as storage on file servers and network bandwidth. Purging stale files and preventing nonbusiness-related streaming video files can reduce storage, backup and bandwidth requirements.
- **Detect rogue/malicious software**—Another key intangible of DLP is identifying malicious software that attempts to transmit sensitive information via e-mail or an Internet connection. Network DLP can help reduce the damage of malicious software by detecting rogue transmission of sensitive information outside the enterprise. This is not always guaranteed since the transmissions may be encrypted. But even in that case, a system that has a rule set that will alert or block data streams it cannot decrypt can prove to be a strong addition to malware defenses.

Risks and Security Considerations

> As with any complex IT solution, implementation of a DLP program, if not managed properly, can present a number of risks to the enterprise.

As with any complex IT solution, implementation of a DLP program, if not managed properly, can present a number of risks to the enterprise. Many of these risks can have a direct impact on business operations, so it is important to take appropriate mitigating steps and keep all business stakeholders involved in this process. **Figure 1** provides a list of the key operational risks related to the implementation of DLP.

---

[4] Ponemon Institue; *Ponemon Study Shows the Cost of a Data Breach Continues to Increase*, USA, 2009, *www.ponemon.org/news-2/23*

Figure 1—Operational Risks Related to DLP Implementation		
Risk	**Impact**	**Mitigation Strategy**
Improperly tuned network DLP modules	• Disruption of business processes • Lost time and revenue • Damage to customer or business partner relationships • Loss of business stakeholder support	Proper tuning and testing of the DLP system should occur before enabling actual blocking of content. Enabling the system in monitor-only mode will allow for tuning and provide the opportunity to alert users to out-of-compliance processes and activities so they may make adjustments accordingly. Involving the appropriate business and IT stakeholders in the planning and monitoring stages will help ensure that disruptions to processes will be anticipated and mitigated. Finally, establish some means of accessibility in the event there is critical content being blocked during off-hours when the team managing the DLP solution is not available.
Improperly sized network DLP module	• Missed or dropped network packets allowing data to pass uninspected	Ensuring that the size of the DLP module is appropriate for the amount of network traffic is a critical design consideration. However, it is just as important to monitor the DLP network modules to ensure that network traffic does not increase over time to a point that renders the module ineffective.
Excessive reporting and false positives	• Wasted staff time • Missing valid threats • Tendency to ignore logs over time	Similar to an improperly configured intrusion detection system (IDS), DLP solutions may register significant amounts of false positives, which overwhelm staff and can obscure valid hits. Avoid excessive use of template patterns or "black box" solutions that allow for little customization. The greatest feature of a DLP solution is the ability to customize rules or templates to specific organizational data patterns. It is also important that the system be rolled out in phases, focusing on the highest risk areas first. Trying to monitor too many data patterns or enabling too many detection points early on can quickly overwhelm resources.
Conflicts with software or system performance	• System down time • Performance degradation • Breaking of DLP or other controls or processes	DLP systems, particularly crawlers and end-point agents, can conflict with other system software and performance. Allowances must be made for ample planning and testing before deployment. Ideally, a permanent testing and staging environment should be available. Check with the vendor for known conflicts. Ensure that crawlers are properly configured and tuned, and that their operation is scheduled in such a way as to avoid peak system processing windows. When avoidable, end-point scans should not be scheduled for peak work hours or when systems are remotely connected. Also ensure that all patches and upgrades are tested within the test environment prior to deployment to production.

Figure 1—Operational Risks Related to DLP ImpLementation *(cont.)*		
Risk	**Impact**	**Mitigation Strategy**
Changes in processes or IT infrastructure rendering DLP controls ineffective	• Reduction of DLP effectiveness due to circumvention of DLP controls	The DLP system administrator or a representative should be involved in change control processes to ensure that changes made do not circumvent or otherwise degrade DLP capabilities. In addition, the enterprise should be well prepared for changes associated with DLP to reduce risk of intentional bypassing of the DLP system in the name of efficiency.
Improperly placed DLP network modules	• Missed or uninspected data streams	It is important to ensure proper placement of DLP network modules. Ensure that accurate network maps are available, and that the modules are placed at the outermost egress point for data flows the enterprise wishes to monitor.
Undetected failure of DLP modules	• Data not inspected due to partial or complete module failure	DLP modules can fail, but do not always report their state to the console. It is important to periodically test to ensure that modules and their associated filters are performing as expected.
Improperly configured or incomplete directory services	• Inability to trace violations to the appropriate end users	The directory service is the key connection between a network address and an actual user, and most enterprises will want to have this process in place as opposed to manual discovery of this information, which can be time consuming and is not always possible. Enterprises that lack or have incomplete directory services should consider addressing this gap prior to implementing a DLP solution.

DLP Limitations

> While DLP solutions can go far in helping an enterprise gain greater insight over and control of sensitive data, stakeholders need to be apprised of their limitations and gaps in DLP solutions.

While DLP solutions can go far in helping an enterprise gain greater insight over and control of sensitive data, stakeholders need to be apprised of limitations and gaps in DLP solutions. Understanding these limitations is the first step in the development of strategies and policies to help compensate for the limitations of the technology. Some of the most significant limitations common among DLP solutions are:

• **Encryption**—DLP solutions can only inspect encrypted information that they can first decrypt. To do this, DLP agents, network appliances and crawlers must have access to, and be able to utilize, the appropriate decryption keys. If users have the ability to use personal encryption packages where keys are not managed by the enterprise and provided to the DLP solution, the files cannot be analyzed. To mitigate this risk, policies should forbid the installation and use of encryption solutions that are not centrally managed, and users should be educated that anything that cannot be decrypted for inspection (meaning that the DLP solution has the encryption key) will ultimately be blocked.

- **Graphics**—DLP solutions cannot intelligently interpret graphics files. Short of blocking or manually inspecting all such information, a significant gap will exist in an enterprise's control of its information. Sensitive information scanned into a graphics file, or intellectual property (IP) that exists in a graphics format, such as design documents, would fall into this category. Enteprises that have significant IP in a graphics format should develop strong policies that govern the use and dissemination of this information. While DLP solutions cannot intelligently read the contents of a graphics file, they can identify specific file types, their source and destination. This capability, combined with well-defined traffic analysis, can flag uncharacteristic movement of this type of information and provide some level of control.
- **Third-party service providers**—When an enterprise sends its sensitive information to a trusted third party, it is inherently trusting that the service provider mirrors the same level of control over information leaks since the enterprise's DLP solutions rarely extend to the service provider's network. A robust third-party management program that incorporates effective contract language and a supporting audit program can help mitigate this risk.
- **Mobile devices**—With the advent of mobile computing devices, such as smart phones, invariably there are communication channels that are not easily monitored or controlled. Short message service (SMS) is the communication protocol that allows text messaging and is a key example. Another consideration is the ability of many of these devices to utilize Wi-Fi or even to become a Wi-Fi hotspot themselves. Both cases allow for out-of-band communication that cannot be monitored by most enterprises. Finally, the ability of many of these devices to capture and store digital photographs and audio information presents yet another potential gap. While some progress is being made in this area, the significant limitations of processing power and centralized management remain a challenge. Again, this situation is best addressed by the development of strong policies and supporting user education to compel appropriate use of these devices.
- **Multilingual support**—A few DLP solutions support multiple languages, but virtually all management consoles support only English. It is also true that for each additional language and character set the system must support, processing requirements and time windows for analysis increase. Until such time that vendors recognize sufficient market demand to address this gap, there is little recourse but to seek other methods to control information leaks in languages other than English. Multinational enterprises must carefully consider this potential gap when evaluating and deploying a DLP solution.

These points are not intended to discourage the adoption of DLP technology. The only recourse for most enterprises is the adoption of behavioral policies and physical security controls that complement the suite of technology controls that is available today, such as:

- **Solution lock-in**—At this time there is no portability of rule sets across various DLP platforms, which means that changing from one vendor to another or integration with an acquired organization's solution can require significant work to replicate a complex rule set in a different product.
- **Limited client OS support**—Many DLP solutions do not provide end-point DLP agents for operating systems such as Linux and Mac because their use as clients in the enterprise is much less common. This does, however, leave a potentially significant gap for enterprises that have a number of these clients. This risk can only be addressed by behavior-oriented policies or requires the use of customized solutions that are typically not integrated with the enterprise DLP platform.
- **Cross-application support**—DLP functions can also be limited by application types. A DLP agent that can monitor the data manipulations of one application may not be able to do so for another application on the same system. Enterprises must ensure that all applications that can manipulate sensitive data are identified and must verify that the DLP solution supports them. In cases where nonsupported applications exist, other actions may be required through policy, or if feasible, through removal of the application in question.

Governance and Change Considerations

Prior to the selection and implementation of DLP technology, it is important to ensure that appropriate policies are developed to govern its use.

The introduction of a DLP solution to an enterprise can impact many IT systems and business processes. These impacts may involve significant changes to long-standing business processes, greater overhead on key systems, and changes to system and network configurations. Prior to the selection and implementation of DLP technology, it is important to ensure that appropriate policies are developed to govern its use. It is also important that DLP policy development involves key business stakeholders who understand what information should be restricted and why. In a recent presentation at a Gartner security and risk management summit, Gartner analyst Eric Ouellett observed:

Organizations underestimate the need for the involvement of non-IT business units. In many instances, it's not really appropriate for IT people to be in the middle of looking at what DLP systems can report about data compliance issues, but the practical use of DLP monitoring sometimes doesn't make it into the hands of the right business people.[5]

The key takeaway is that the correct business people should be involved in the initial policy development as well as when the DLP program is live because they will be critical in making judgment calls regarding violations. The business data owner who has an idea of the context is far more equipped to make these decisions than an IT security analyst. It is also important that these stakeholders fully understand the ramifications of the expected changes and that there be appropriate preparation to avoid a negative impact to the business processes.

It is also important to recognize that significant changes to business processes or longstanding procedures can have broader cultural impacts to the enterprise. Despite best efforts to communicate and educate prior to implementation, some individuals may not understand or accept the changes and may seek ways to circumvent the new controls, introducing additional risk to the enterprise. Understanding the systemic nature of information security management, such as that described in the ISACA research publication *An Introduction to the Business Model for Information Security,*[6] can assist in the development of strategies to address this risk.

Enterprises should ensure that a risk-based approach is utilized when implementing a DLP solution. Even when deployed in a monitoring-only mode, it is easy to be overwhelmed with the amount of information presented by the system. When this occurs, there is a distinct possibility that the solution will either be tuned down to the point that it is ineffective or will eventually be ignored, as was the case with many early intrusion detection systems (IDSs). An approach that some enterprises are taking is implementing DLP only for specific systems or protocols that they have determined to be at high risk. A single channel frequently covered is e-mail since it often poses the single greatest data loss risk to an enterprise.

Assurance Considerations for DLP

Assurance professionals have the task of ensuring that the DLP solution is properly deployed, managed and governed.

Assurance professionals have the task of ensuring that the DLP solution is properly deployed, managed and governed. This involves having a clear understanding of the risks as well as ongoing monitoring of four key areas:
- **Enterprise strategy and governance**—Review the data protection strategy to examine whether it is in line with the business objectives and risks. Pay attention to indirect risks where confidential information may be abused by

---

[5] *Network World*; "Too many data-loss prevention tools become shelfware, says analyst," 22 June 2010, *www.networkworld.com/news/2010/062210-data-loss-prevention-tools.html*
[6] ISACA; *An Introduction to the Business Model for Information Security*, USA, 2009, *www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf*

competitors. Assess whether there are checkpoints to keep data strategy aligned with changing business objectives. Verify whether a clear governance framework is in place to orchestrate actions across people, process and technology. Verify whether all applicable regulations, legislation, and privacy laws are considered.

• **People**—Verify whether appropriate stakeholders are engaged during and after DLP implementation. Key stakeholders include:

  – Legal, privacy, corporate security, information security
  – IT engineering and operations
  – HR and employee representatives
  – Key business line representatives
  – Executive management

  Review the training and awareness program to ensure that employees are aware of their roles and responsibilities. Ensure that staff required to handle confidential information is properly trained according to the enterprise's security policy and that only staff with a business requirement has access to confidential information. Also ensure that the appropriate stakeholders are involved in the identification of sensitive data and the workflow that evaluates and addresses DLP policy violations.

• **Business process**—Review business processes with access to confidential information and determine whether that access is required to perform each process. Identifying the need for access to confidential information from business processes is one of the strongest methods of protecting such data. In addition, appropriate processes for monitoring, detecting, qualifying, handling and closing data leakage incidents should exist.

• **Technology**—Review the specific technology that has been deployed and determine whether it is installed as designed. For example, determine whether it covers all egress points and devices critical to the enterprise. This should include business partner egress points and devices with access to sensitive information. In addition, ensure that it covers all of the required elements of the technology in use at the enterprise. Finally, periodic reviews of logs and event handling processes ensure that the solution is being utilized in an appropriate and optimized manner.

Conclusion

An enterprise's information can be among its most valuable assets. DLP solutions offer a multifaceted capability to significantly increase an enterprise's ability to manage risks to its key information assets. However, these solutions can be complex and prone to disrupt other processes and organizational culture if improperly or hurriedly implemented. Careful planning and preparation, communication and awareness training are paramount in deploying a successful DLP program.

> DLP solutions offer a multifaceted capability to significantly increase an organization's ability to manage risks to its key information assets.

Additional Resources and Feedback
Visit *www.isaca.org/dlp* for additional resources and use the feedback function to provide your comments and suggestions on this document. Your feedback is a very important element in the development of ISACA guidance for its constituents and is greatly appreciated.