

## A N A L Y S T C O N N E C T I O N



*Eric Damage*  
*Program Manager, Western European Security Products & Solutions, IDC*

### **Taking Back Control of Information Flow — Why Organizations Should Implement DLP**

*June 2009 — Sponsored by Symantec*

*Recent volatility on financial markets has raised many questions about how the global economy will recover from the downturn. Many organizations and individuals fear a deep impact on our economies, and the crisis could last longer than just a few months.*

*In such a depressed environment, organizations and individuals must maintain key protective actions: business continuity, data security, and robust IT are the foundations of a recovering economy. No trade-off is possible on security, and organizations must stay carefully focused on their own security during times of turmoil. In a crisis, the robustness of an organization is challenged from all sides. The challenges of the downturn itself, of agile and aggressive competition, hacker attacks, and the misuse of IT are bringing complexity to daily business life.*

*How can organizations deal with this pressure?*

*One of the many responses to this question is with robust IT and data, which appears to be the key strength for a safe recovery. Many areas need to be protected and ruggedized: IT infrastructure must be resilient, seamless, and adaptive; applications must be available and free of breaches; access to information must be easy but strictly filtered; and the use of connected IT must comply with internal and external regulations.*

*Above all, information and data are seen as currency for organizations. The flow of information irrigates the business and operational parts of organizations, just as currency irrigates economies.*

*New security solutions have been developed to secure data while in transit, while being used, or while being stored — namely data loss prevention solutions.*

#### **Q: What value does data loss prevention (DLP) deliver to organizations?**

**DLP solutions bring real innovation to the protection of an organization.**

DLP addresses business issues and delivers business solutions; this is the first time that a security solution has truly addressed a business problem instead of a technical problem.

DLP allows organizations to set up, operate, and distribute an effective security policy for information flow in order to keep control of critical information (e.g., blueprints, financial metrics, source codes), prevent accidental breaches of compliance and confidentiality policy (e.g., privacy breaches, non-disclosure agreements, confidentiality), and support the user's ubiquity while using laptops or smaller devices.

On a policy level, DLP:

- **Assesses information**, whether structured or unstructured

- **Creates policies to detect and protect** that information while in use, at rest, or in transit. IDC recommends focusing on a few basic data types during the early stages of a DLP implementation. For example, EU privacy rules require the protection of personal identifiable information (PII) and PCI-DSS (Data Security Standard) regulations require rigorous protection of credit card details, so start by creating policies to protect personal data and credit card information. In the vast majority of situations, all personal data and all credit card details should be protected, without question.
- **Applies policies** to storage repositories, network gateways, and endpoint machines — online or offline — to determine policy violations, and provides real-time remediation and notification to impede data from leaving the organization inappropriately.

Since DLP addresses a business challenge, a mature DLP solution also drives information security responsibilities back to the business data owners and provides employees with real-time education about information security policies, giving ownership of data protection to the entire enterprise.

### **Q: Where does DLP fit with other data security solutions?**

The primary business benefit of a DLP solution is that it provides visibility into the location of an organization's data loss risk and offers the tools to lower that risk. By providing intelligence on the location of risk areas, DLP can act as the cornerstone of an organization's security strategy by bringing together and prioritizing the implementation of other security solutions such as encryption, digital rights management, and watermarking.

DLP is a set of solutions that goes beyond existing security solutions to protect information while in use, in motion, or at rest. DLP differs from many other technologies in that it begins with an assessment process in which content inspection is key. Unlike other data protection technologies, DLP looks inside files wherever they are (in use, in motion, or at rest), allowing real information security beyond just context security (e.g., file-type-only discovery and security). For example, DLP solutions discover credit card numbers in any kind of file (e.g., .doc, .xls) and generate specific actions (alert, block, event collection) based on the severity of the credit card violation.

Unlike other data protection solutions, DLP also addresses the fact that the majority of data loss is accidental. Solutions such as encryption protect a laptop if it is stolen or lost, but do not address the most common data loss situations caused by people who have legitimate access to an organization's sensitive data.

The DLP solution set is used in three different situations:

**Data-in-use.** Data-in-use DLP includes solutions that protect and control information in use at the endpoint. These solutions are used to protect sensitive information such as contracts, term sheets, and other business-critical documents as they are being used on or off the network. For example, DLP can prevent an end user from copying sensitive data from their laptop onto a USB drive or printing it out while connected to their home network.

**Data-in-motion.** Data-in-motion DLP includes solutions that monitor, encrypt, filter, and block outbound content in email, instant messages, peer-to-peer transactions, file transfers, Web postings, and other types of messaging traffic. For example, DLP can detect and take protective action on a specific email containing classified information while allowing other emails with non-confidential data to be sent out.

**Data-at-rest.** Data-at-rest DLP includes solutions that discover, protect, and control information on servers, databases, desktops, laptops, file/storage servers, USB drives and other types of data repository. DLP helps find internal "data spills" and then starts to clean them up, thus reducing risk.

As DLP is a policy-driven solution, one primary benefit of a mature DLP solution is that it can centrally manage policies, remediation, and reporting to ensure that an organization's critical information is protected, whether it is in use, in motion, or at rest.

**Q: Given current economic conditions, is DLP a solution that organizations should consider?**

Although the majority of data loss is perpetrated by well-meaning insiders, lean economic times often result in redundancy plans that create employee anxiety and frustration. It is also critical to understand that any holes in securing routine processes can generate major business impacts. Therefore, DLP is a solution that should be considered now, as it will support stronger security in the following areas:

■ **Managing the Insider Threat**

- In the U.K. alone, almost 10,000 jobs were lost in the financial industry in 2008 due to the financial crisis. In such a context, all organizations must take control of the insider threat generated by personal frustration. Personal retaliation against a company has never been easier, given the expansion of IT in industry. Data theft, intentional misuse of IT tools, and IT attacks from inside organizations will be a major threat in 2009, given the current economic context. DLP can help assess an organization's critical data and prevent misuse of such assets in a complex crisis.

■ **Doing More With Less**

- **Enhanced and secured ubiquity.** Always-on secured and available users are a competitive advantage. User productivity and agility to react swiftly and securely to market needs is an advantage. DLP enables always-on and ubiquitous work by securing and controlling information flows wherever the user is.
- **Centrally monitored security policy and enforcement.** With DLP, automated enforcement processes eliminate the need for the user to manually enforce information security and compliance requirements. The DLP console is centrally managed under a global IT policy and provides workflow capabilities that distribute the responsibility of data protection to the *entire business* so that business units can set rules and manage enforcement. In a general context, DLP acts as a global responsibility tool with which business owners can act directly on security.
- **Always-on compliance.** Information leakage often breaches regulations, and the most common data leakage violations breach EU privacy obligations. Others breach industry norms such as financial regulations and PCI-DSS. DLP helps organizations protect critical information to maintain compliance with privacy, PCI-DSS, or other data protection regulations.

**IDC Recommends**

- To begin with, organizations should ask PR offices and brand reputation agencies to tell them how much undesired information is already outside the company. Very often, the results can be surprising. Web 2.0 penetration and personal posts by employees can demonstrate a very low level of education about key security behavior in the organization. The first step is often the most alarming, simply because it provides a real idea of the problem to be addressed.
- Save your time! At the start of a DLP project, organizations should review simple regulations to initiate their implementation strategy. For example, EU privacy rules, whatever the country of application, require the total protection of any personal identifiable information (PII). So all PII should be assessed, protected, and monitored. PCI-DSS mandates full protection of credit card numbers, and data should be protected appropriately. IDC recommends starting with these very basic, broad, and easy DLP policies instead of drilling down into complex legal considerations. Fine-tuning can take place after the initial implementation.

- DLP-experienced organizations have seen a major reduction in data breaches shortly after implementation. In fact, DLP solutions will very quickly change users' behavior by alerting them to the misuse of critical data. In some cases, the volume of data breaches could be halved in a very short time. However, this does not mean that DLP will eliminate data leakage in a single shot. DLP policies are a continuous process that requires an iterative approach to assessment, rules and policies, and monitoring and enforcement.

#### ABOUT THIS ANALYST

*Eric Damage is program manager with IDC's European Software and Services Group, and is responsible for managing the European Security Products and Solutions research and consulting. Specific research areas include market analysis, competitive analysis, market dynamics, vendor activities, and end-user trends.*

---

#### ABOUT THIS PUBLICATION

IDC Go-to-Market Services produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

#### COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or [gms@idc.com](mailto:gms@idc.com). Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit [www.idc.com](http://www.idc.com). For more information on IDC GMS visit [www.idc.com/gms](http://www.idc.com/gms).

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 [www.idc.com](http://www.idc.com).