

EXECUTIVE BRIEF

Business Value of Data Loss Prevention

Sponsored by Dimension Data

Eric Damage
Jozef Gemela
September 2009

EXECUTIVE SUMMARY

Data loss prevention (DLP) solutions represent sophisticated systems that help organizations keep control of confidential information, and they help to avoid accidental or malicious leakages of sensitive data inside and outside of the organizations. DLP is a set of IT security technologies, internal processes, and intelligence and risk management tools for monitoring and protecting data in use (information at the endpoint), data in motion (outbound content), and data at rest (data repositories). DLP addresses both intentional and unintentional data loss incidents, prevents breaches in regulatory and internal policies, and helps organizations meet compliance requirements.

The primary driving forces behind the adoption of DLP solutions are the protection of intellectual property (including corporate brands) and regulatory compliance. DLP represents a business solution and addresses business issues as opposed to technical problems. Data loss is not only a problem for data-sensitive industries; it spans all business sectors.

DLP is data-centric and includes IT technologies, processes, policies, and people. DLP does not represent a new revolutionary concept that disrupts existing business models or IT plans. Instead, it is a combination of existing best-of-breed solutions built around all data loss vectors.

Considering the link to underlying business issues, IDC recommends that organizations not only concentrate on basic perimeter security but also focus on more advanced and comprehensive business protection. Data is the currency, and thus security needs to be data-centric, reflecting and serving the underlying business issues.

The link between DLP solutions and business needs, with a need for customization to reflect the respective company specifics, also stems from the fact that data loss threats are perceived differently by various business sectors. Hence, in order to develop and deploy a functional DLP system, a balanced portfolio of consulting, implementation, and managed security services needs to be considered.

Despite the current economic turmoil, IT security and DLP remain on the list of the top IT investment areas, as security investments represent a key enabler for collaboration, productivity, and compliance.

METHODOLOGY

IDC developed this executive brief using a combination of existing knowledge and market studies and direct in-depth primary research. To gain insight into the

challenges of preventing sensitive information from leaking through corporate boundaries, IDC conducted an extensive on-line end-user survey among 407 organizations across 18 countries, covering Western Europe, the Americas, the Middle East, Africa, and Asia/Pacific. Only companies with more than 500 employees were interviewed.

IN THIS EXECUTIVE BRIEF

This executive brief looks into the current situation and needs in the segment of IT security, with a special focus on the business value of DLP technologies. It provides an overview of the DLP issues facing organizations in their day-to-day business operations and a summary of solutions designed to tackle the security threats in this field.

SITUATION OVERVIEW

Revolution in the Productivity Area

The tremendous connectivity expansion IDC has witnessed over the past decade represents one of the major trends bringing new opportunities and challenges into today's business and social environments. We live in the ever-electronically connected world. Whether in the office, at home, or on the road, we remain constantly connected.

What is the main driver spurring the growth in electronic connectivity in the business environment? IDC is of the opinion that the major driver stimulating demand for higher connectivity is the need for collaboration. Agile organizations have entered the collaboration age. Remote/Mobile access to ERP systems, email and messaging systems, mobile applications, and IT and business outsourcing are examples of technologies and business concepts enabling intensified collaboration among internal and external stakeholders.

The collaboration age represents the next revolution in productivity. Intensified collaboration is vital for increasing the productivity of the workforce. Connectivity stays critical, but collaboration is the new business enabler. But how could collaboration work without trust, security, and continuity at all stages covering networks, users, and data? While the connectivity-collaboration-productivity value chain is becoming the key business enabler, IT security is becoming the support factor for all business operations. No IT security means no collaboration, no productivity, and no business.

IT Security Budgets Under Pressure

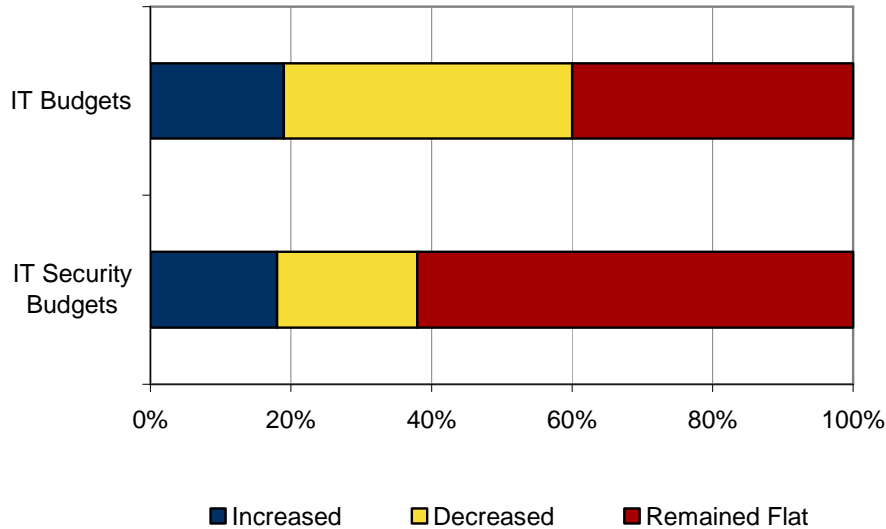
The economic crisis is leading to IT spending cuts across most product groups, segments, and sectors. Key trends in the market include a strong focus on cost controls and efficiency planning, replacement cycles being extended, renewal of OS and application software being postponed, and planned reductions in IT personnel. In the current volatile climate, IDC has witnessed strong growth variations between and within countries, products, segments, and sectors.

In such a depressed environment, organizations and individuals must keep up with key protective actions – business continuity, data security, and IT robustness. According to a survey conducted by IDC, IT security remains on the list of the top IT

investment priorities. As Figure 1 below indicates, while 41% of surveyed companies plan to cut their total IT budgets in 2009, only 20% of them plan to decrease their IT security spending.

FIGURE 1

IT and IT Security Spending Changes, 2009 vs. 2008



Source: IDC, 2009

Despite the current economic turmoil, IT security still remains on the radar of IT and business managers. IDC is of the opinion that the positive attitude toward IT security lies in the following drivers:

- Support of the connectivity-collaboration-productivity value chain
- Increased proliferation of notebooks and mobile devices
- Greater likelihood of sensitive information being stolen or disclosed by workers made redundant during these times of massive layoffs
- Sensitive information threatened by mergers and acquisitions

DATA LOSS PREVENTION

What is DLP?

DLP enables organizations to set up, operate, and distribute an effective security policy for information flow (internal and external) in order to keep control of critical information. Two principal forces drive the use of DLP: protection of intellectual property and regulatory compliance. DLP enables organizations to prevent accidental breaches to regulatory or internal policies (e.g., privacy, non-disclosure agreements, and confidentiality) and supports each user's mobility while using a laptop or smaller device. DLP applies to the following information areas:

- ☒ **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.
- ☒ **Data in Motion:** Data-in-motion DLP includes solutions that monitor, encrypt, filter, and block outbound content contained in email, instant messaging, peer-to-peer, file transfers, Web postings, and other types of messaging traffic.
- ☒ **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 repositories.

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

Cost of Data Losses

DLP is a complex problem comprising IT security technologies, internal processes, compliance requirements, intelligence, and people, and it applies to both intentional and unintentional data loss incidents. Data loss is no longer a problem of data-sensitive industries only (e.g., of finance and healthcare); it spans all business sectors. Organizations and governmental bodies collect and store sensitive information about customers, sales transactions, contracts, employees, and intellectual property. This information is often shared with third parties, and thus the ultimate goal of chief security officers is to keep control of the data flow and avoid data transfers to unprotected locations.

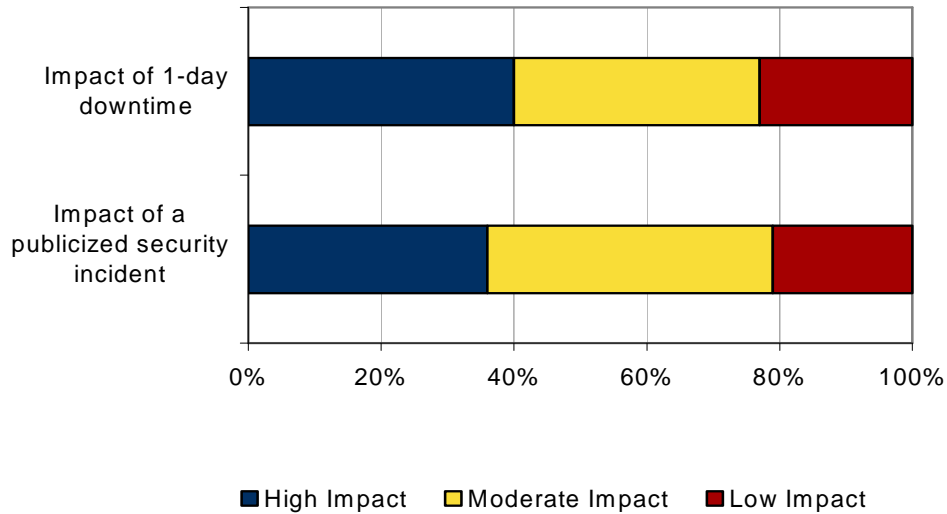
Data loss risks arise from both internal and external sources, and the consequences of information leaks can be distressing, as it can include financial losses, recovery costs, penalties, lawsuits, negative publicity, damage to the organization's reputation and good name, and threat to public security.

Given the wide range of tangible and intangible data loss-related costs, it is very difficult to quantify the total financial impact of data breaches. In addition, the consequences of such accidents might not be immediate. A lost blueprint or divulged customer or financial data can trigger competitive activities that cannot be measured just a few days after the data leakage.

However, to address this question, IDC compared the perceived impact of publicized security incidents with the impact of one day's downtime. Figure 2 suggests that the perceived impact of both incidents is almost identical. In many enterprises, the impact of one day's downtime on a company's business could be destructive, and the impact of publicized security incidents is perceived in a similar way.

FIGURE 2

Perceived Impact of Incidents on a Company's Business



Source: IDC, 2009

Data Loss Threats and Threat Mitigation

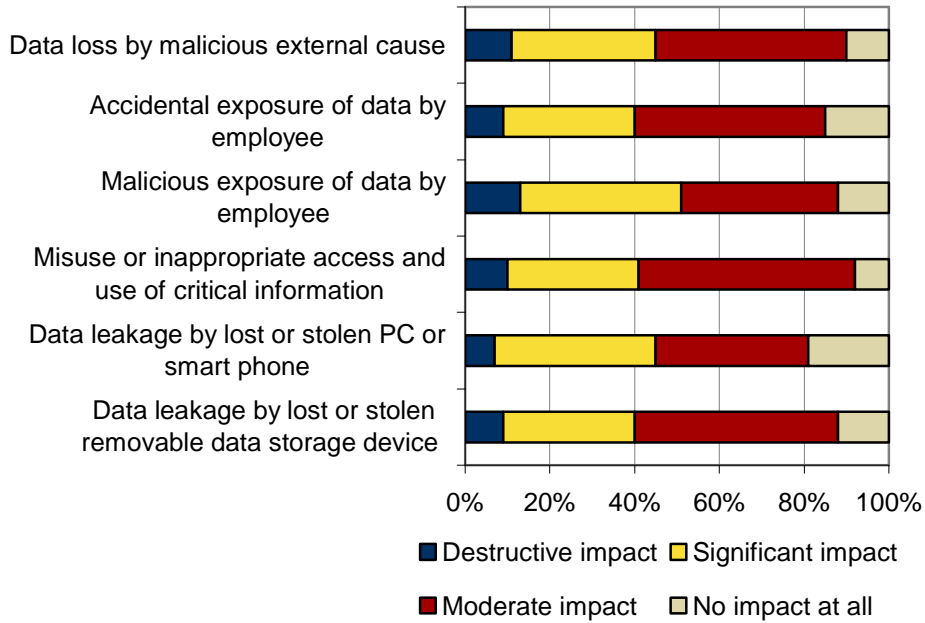
Data loss threats encompass a wide range of incidents, including accidental and malicious exposures. According to the IDC survey, data loss threats are understood to arise from both mistakes in usage and intentional actions. As Figure 3 below displays, surveyed organizations fear both accidental and intentional data loss incidents. "Malicious exposure of data by an employee" represents the biggest threat –51% of surveyed organizations stated that this incident would have a destructive or significant impact on their businesses. Other critical threats are seen to be "data leakage due to a lost or stolen PC" and "data loss due to a malicious external cause," for which a destructive or significant impact was foreseen in 45% of the interviewed organizations.

According to the survey, data loss threats are perceived differently in various business segments:

- ☒ In general, in very large enterprises (with more than 1,000 employees), the level of fear is lower due to higher adoption of DLP technologies. Among other threats, "malicious exposure of data by an employee" is the top concern, with 52% of organizations indicating a destructive or significant impact.
- ☒ Large organizations (500–1,000 employees) fear hacking in particular ("data loss due to malicious external cause"). For 55% of the interviewed organizations, this threat is perceived to have a destructive or significant impact.
- ☒ In the data-sensitive finance sector, half of companies are concerned about "accidental exposure of data by an employee," whereas other vertical markets indicated "malicious exposure of data by an employee" as the threat with the most destructive or significant impact on business.

FIGURE 3

Perceived Impact of DLP Incidents on Organization



Source: IDC, 2009

DLP: A Reality Check From the Field

DLP does not offer a simple packaged solution; DLP efforts should be adapted to specific business needs. Due to market diversity, various business sectors show different portfolios of emerging data loss threats. DLP thus requires an optimal combination of best-of-breed solutions, taking into account the following recommendations:

- ☒ DLP is data-centric and should include IT technologies, processes, policies, risk management, and people.
- ☒ DLP solutions should be based on a detailed risk-assessment exercise that examines all forms of data flow (data in use, data in motion, and data at rest) in order to identify and eliminate all data loss vectors and create an unbreakable chain of security links.
- ☒ Implemented DLP solutions should align with governance, risk, and compliance (GRC) policies. DLP should be configured to support GRC standards and not to compete with them. Conversely, GRC can rely on DLP and create standards for security deployments.

When implementing or deploying a DLP solution, a number of obstacles and challenges need to be considered. The most significant are as follows:

- ☒ DLP often means troublesome changes of complex organizational processes.
- ☒ DLP affects processes and user workflows, which creates resistance to change. User cooperation is vital to the success of DLP.

- ☒ DLP requires integration of complex IT infrastructures in multi-vendor environments.
- ☒ Business units need to play the key role in defining the role of DLP. DLP and GRC should be fully aligned.

DLP remains one of the top priorities for organizations, as it is necessary for protecting intellectual property assets and is instrumental in helping companies comply with regulations. According to the survey, 92% of organizations claim they either currently use or plan to adopt DLP models within the next 12 months. When considering development or deployment of DLP solutions, a blend of the following security services should be considered:

- ☒ **Consultancy:** This focuses on understanding and planning strategic and operational actions for eliminating data loss by using standard or proprietary consulting frameworks with emphasis on proper risk assessment.
- ☒ **Implementation:** This involves taking action on DLP risks, which include technology, people, and processes, and filling in the gaps where vulnerabilities remain.
- ☒ **Managed Security Services:** These are about supporting and handling security complexity, including resource scarcity. The services offer onsite and remote management of information security, with real-time monitoring, protection, escalation, and response processes.

All discussions and propositions in the DLP area must include consideration of the cost factor (cost reduction or cost control) as a central, compulsory, and main concern for organizations. Organizations are looking for solution-oriented DLP services rather than problem-oriented ones, and thus the key benefits of DLP should include:

- ☒ Centrally managed security policy for the entire infrastructure
- ☒ Insider threat management
- ☒ Enhanced and secured mobility
- ☒ Compliance

All DLP business models should generate ROI, control data flows, and support business operations in tandem with engendering positive opinions on success enablement.

CONCLUSION

While DLP represents a complex system in its post-hype lifecycle period, there is nothing revolutionary behind the concept. It is a combination of best-of-breed solutions aimed at data leakage risks and targeting IT technologies, processes, people, and compliance requirements. Most concerns and threats are known to organizations and are not necessarily linked to a specific DLP strategy.

The objective of any DLP system should be to mitigate risks, reduce costs, generate ROI, and focus on business solutions instead of technical problems.

IDC recommends that organizations do their homework to ascertain their data loss risks. Where substantial risks are identified or compliance regulation is required,

appropriate DLP solutions can close security or compliance gaps, bringing peace of mind to IT and business managers, as well as to the wider management team, which can then feel secure that the company's intellectual property and other sensitive data will not be compromised.

Dimension Data Profile and Offerings

Founded in 1983, Dimension Data is a reputable provider of IT solutions and services focused on IT infrastructures, including security and DLP solutions. During more than 25 years of existence, Dimension Data has established a global footprint, with a direct presence in 47 countries and serving clients in many more. The organization has established strategic partnerships with global IT vendors that include Cisco and Microsoft. Dimension Data's vision is to become a world leader in the provision and management of specialist IT infrastructure solutions that help clients to achieve their business goals.

In the area of IT security, Dimension Data offers a wide range of services, taking a consultative-led approach. The company's engagement process covers the following phases:

- ☒ Compliance and risk assessment
- ☒ IT security strategy and planning
- ☒ Designing and building infrastructure
- ☒ Implementation and integration of IT security solutions
- ☒ IT security operations management

FIGURE 4

Security Solutions Approach



Source: Dimension Data, 2009

The engagement framework focuses on assessment, planning, and implementation of infrastructure, as well as procedures and measures to optimize the IT security environment and to achieve and maintain compliance with local and global regulations. This is realized through understanding and examining the broader IT infrastructure components, including the network, endpoints, perimeters, and applications and the data itself. IT security solutions are built in cooperation with global strategic vendor partners, including Cisco/IronPort, Blue Coat, Check Point, Fortinet, McAfee, and RSA.

In terms of DLP, Dimension Data focuses on data-centric business solutions that address the inappropriate and unauthorized use of information. As data can take different forms and can be found in various contexts, the company takes a holistic approach and offers solutions covering data at rest (stored on endpoint devices or centrally) and data in transit (traversing the network), as well as data beyond organizations' boundaries. Dimension Data's offerings relevant to IT security – and to DLP in particular – represent a balanced proposition that addresses emerging IT security challenges and covers the full range of IT security technologies, architectural components, and relevant security services.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. Copyright 2009 IDC. Reproduction without written permission is forbidden.