



DATA LOSS PREVENTION VITAL TO PROTECTING YOUR COMPANY & CUSTOMER INFORMATION

COSTS OF DATA LOSS INCIDENTS

The damage to a company's reputation and brand and resulting loss in customer trust and business from a data loss incident can be substantial. According to a leading research firm, The Ponemon Institute, the average information leak today costs organizations approximately \$202 per record, averaging roughly \$6.6 million per breach in total.

DATA LOSS PREVENTION REDUCES RISKS WHILE HELPING TO DEMONSTRATE AND ENFORCE COMPLIANCE

Data loss prevention (DLP) describes the varied and increasingly important methods companies are adopting to ensure that corporate and customer information is not lost or inadvertently sent outside or misused inside an organization. Along with the vast growth in the amount of electronic data an organization must collect, store and manage, the traditional network perimeter and workplace boundaries have virtually disappeared in today's Internet connected and highly collaborative world.

The concept of protecting data and information is not new, and organizations have implemented risk mitigation and security initiatives like data classification, identity and access management, and defense-in-depth strategies for years with variable levels of success. However, the challenge of achieving comprehensive protection of company and customer information while minimizing the costs associated with data loss incidents, has elevated data loss prevention to a major business priority.

As a result, companies are re-examining their information management and security postures, and corporate goals increasingly reflect a heightened responsibility for establishing stronger controls around the management of data assets. Recognizing the urgency and importance of DLP, companies are seeking ways to monitor and protect all data that's moved or stored throughout an organization. They are looking for solutions that help to reduce risk, manage employee behavior, and demonstrate compliance with regulations and policies in today's environment of limited IT resources and constricted budgets.

Threats and regulations drive data protection efforts

Nearly every organization has confidential data of some kind and/or intellectual property and data of strategic corporate value that must be protected from misuse and threats, and to sustain and ensure the company's competitive edge. Because data is now embedded in every aspect of business operations, it has become the currency of the modern enterprise and must be protected as a critical asset.

THE MAJOR CAUSES OF DATA LOSS

INTERNAL

Lack of Awareness/Negligence

In a context of trying to accomplish more with less, data disclosure occurs most often due to people's lack of awareness and failure to abide by policies, and their unintentional misuse of technologies. For example, sensitive information may be transmitted electronically outside an organization's network via email, instant messaging, blogs, chat rooms, and is often not monitored. Lost laptops, PDAs, flash drive sticks, and even iPods can contain highly sensitive but unprotected data.

Systemic Risk

Data disclosure occurs due to lack of policies and standards or from faulty business processes. Common risks include the lack of visibility into where sensitive data is stored, the lack of understanding around who has access to sensitive data, and the lack of secure storage for sensitive data to prevent theft and loss.

Malice/Retaliation

Disgruntled, bribed or terminated employees can deliberately steal or misuse sensitive information, and recent research has indicated that terminated employees often take information with them when leaving a job.¹

EXTERNAL

Hackers and Spammers

These individuals or groups can gain access to or control of a system to facilitate stealing proprietary information as well as manipulating IT systems for conveying spam or future attacks.

Organized Crime

Criminal enterprises steal data from vulnerable systems to sell to others, use in fraud schemes, or even to blackmail organizations with the threat of releasing information to the public or over the Internet.

With hundreds of millions of records reported lost or stolen in 2008, according to a recent Verizon Communications study,¹ companies have to be concerned about data loss from a wide range of sources. These include mobile computing devices (laptops, PDAs), data and voice convergence devices (e.g. Blackberry), and business activities such as outsourcing and offshoring. In addition, the risks of losing or misusing sensitive data have grown as companies increasingly share information with business partners, suppliers and other service providers across the Internet.

Data loss prevention solutions have emerged to directly address threats from the sharing, transmission and storage of information assets through a multitude of vehicles and channels. Companies can now get a clearer picture of the location and exposure of stored confidential data, the volume and types of data leaving their networks, and the methods, frequency and nature of data transmitted outside their organizations. Armed with this insight, companies can quantify and qualify risks associated with information assets as well as mitigate risks and eliminate costs from data breaches or incidents.

At the same time new regulations and laws governing privacy and data handling have emerged that require special attention to securing information assets, including internal and external audits to verify compliance. Several U.S. and international regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI) Data Security Standard and the European Union Data Directive require companies to safeguard customer and other company information. Demonstrating compliance with multiple regulations as well as internal policies now consumes a significant portion of IT resources and staff time for companies across the globe.

Data loss prevention solutions can now provide visibility into information assets that indicates what, if any, regulations or policies may have been violated over a given period of time, as well as monitoring individuals or groups with permissions to access specific kinds of sensitive information. DLP solutions also encompass policy-driven data discovery, monitoring and automated prevention measures that help to enforce compliance as well as demonstrate compliance for audit purposes.

Putting a dollar value on data loss prevention

What is the trade-off between efforts expended to protect sensitive data and the consequences of data loss? A recent study from the IT Policy Compliance Group, a consortium of leading audit, security and compliance organization, has helped to quantify some answers.³

Research conducted with 2,600 firms shows that 68 percent of firms are under-spending on information security relative to the financial risks and losses they are experiencing. Yet incremental increases in funding best practices are responsible for financial returns that can exceed more than 200 percent for most organizations.

A leading analyst firm reports that 70 percent of security incidents involving data loss are caused by insiders such as employees or contractors. However, most incidents do not occur because of malicious intent, but rather from unintentional mistakes and misunderstood policies.⁴ This suggests that modifying employee behavior with automatic notifications of policy violations and awareness training are essential to reducing risks of data loss from inside the organization.

Among organizations with \$5 billion in revenue, the combined costs from data loss or theft and business downtime ranged from \$329 million for firms with the worst practices to \$2.25 million for firms who had implemented the best practices. That's nearly 150 times less.

The research also found that firms with the best outcomes for protecting data were actually spending between 35 and 52 percent less on audit fees and expenses. For these firms, adjusting the amount of money spent on practices that reduce risk, loss and audit spending produced financial returns ranging from 1,000 to 500,000 percent more than the loss which the organizations are willing to risk sustaining.

Research director at the ITPCG, Jim Hurley summed up the research results by saying, "Firms can either wait until an emergency pushes them to reprioritize, or they can decide that it is in their best interests to institute industry proven practices."

Minimizing risks and improving operations with DLP

The benefits of implementing data loss prevention can add up to significant amounts of cost avoidance, minimizing potential damage to customer relationships and brand reputation, and reducing legal liabilities. This enables an organization to improve its overall management and use of critical business information assets for competitive advantage.

DLP solutions help to strengthen customer and shareholder confidence by improving the ability to protect intellectual property and the privacy of customer data. This helps avoid any negative impact on analyst or shareholder confidence that could be devastating to an organization's value.

By reducing the number and severity of incidents of data loss, DLP solutions help organizations avoid or minimize the expense of remediation costs while enforcing adherence to existing corporate and regulatory policies for data usage.

By providing visibility into an organization's risks as they relate to data flows and data usage, DLP solutions provide an accurate and actionable picture of the organization's overall security and risk posture. In addition, DLP solutions help educate users and influence their behavior through new technologies that automatically notify users of policy violations.

Just as important, a DLP solution makes good governance a reality by helping to increase compliance with evolving corporate policy, regulatory and legislative requirements. Because of growing concerns, public, state and federal regulators in the U.S. are starting to impose stronger controls over customer and patient data. There are, in many cases, state privacy laws that require companies to send security breach notifications to any and all affected parties.

“Current policies designed to protect organizations against the leakage of sensitive information are not considered effective by the majority of organizations,” according to the Messaging Policy Management Trends Report, 2007-2010 by Osterman Research.

Build or buy? The path to an effective DLP solution

As awareness of the costs and benefits of data loss prevention has grown, organizations are budgeting for solutions yet often find themselves struggling to define DLP and how best to achieve it for their specific business model and industry. As part of this process, it's important to weigh the difference between attempting a do-it-yourself approach to DLP, and looking to an outside, third-party to help implement or actually provide DLP as a managed service.

One of the most powerful arguments for considering outside help to plan and implement a DLP solution is that many organizations simply don't have the in-house expertise or ready resources for the task. Because a DLP solution involves more than simply deploying technologies, enterprises may want to take advantage of third-party expertise and experience in managing the cultural changes, process design and deployment, and controls needed for a successful implementation.

In almost all cases, organizations that consider deploying a DLP solution need to first get an objective picture of their current DLP posture and what specific risks they may be facing. To start the process of developing a solution, organizations have to decide what data is most important to protect, and identify who is touching that information. Organizations also need to know which communication channels and vehicles pose the greatest risk of data loss, and what policies apply. They have to choose the most effective and appropriate technologies and determine what to monitor and how to enforce compliance.

Answering these questions often requires an engagement performed by an outside, “objective” third-party designed to identify and prioritize sensitive data and the security posture surrounding it, in order to determine recommendations for an effective DLP solution.

Why CSC should be considered a first step

When developing a DLP solution, organizations must typically satisfy several goals: brand value preservation, customer privacy protection, retaining intellectual property, and compliance with policies and regulations. The most desirable and cost-effective solutions will accelerate the DLP adoption process to protect business data, avoid data breaches and their consequences, and allow IT to focus on delivering business value. CSC is a leader in offering proven, practical methods and services to manage the people, processes and technologies involved in a successful DLP program, including:

- The ability to help organizations properly identify and analyze their data security and protection needs
- Transition and transformation services to help organizations quickly and efficiently realize the benefits of DLP within their organization

CSC AND SYMANTEC TEAM UP TO PROVIDE A WORLD-CLASS DLP SOLUTION

The combined strengths and capabilities of CSC and Symantec offer the widest range of options in developing and managing a successful data loss prevention solution. Whether an assessment of your overall enterprise data protection needs, implementing Symantec's best-in-class DLP platform technology in-house, or turning to a trusted advisor for a fully managed end-to-end DLP service; our offerings can be tailored to suit your specific requirements and budget.

- An upfront consulting engagement to identify and prioritize sensitive data, perform business risk analysis and develop a data loss prevention strategy
- A complete implementation of appropriate technology for server, storage, endpoint, and email monitoring and/or protection
- Centrally managed monitoring and protection of sensitive data
- Fully integrated collection, storage, monitoring and protection of sensitive data
- Detection and alerting of critical incidents and rapid response, including automated workflow
- Flexible architecture to tailor service to your unique needs, backed by full scope of consulting and managed services

People: With unmatched experience in managing the security and systems of all sizes of organizations across the globe, CSC has a wealth of consulting services and hands-on technology experts with in-depth insights into the demands of specific industries and environments. From healthcare, to insurance, manufacturing to retail, and government to transportation, CSC offers skilled and qualified consultants to assist organizations in defining appropriate policies and approaches to implement a successful DLP solution.

Process: As a leader in complementary managed services, CSC has the advantage of years of refining processes that reinforce each other among critical data protection areas to help organizations:

- Gain an understanding of the data lifecycle with ongoing data flow and gap analyses, helping to understand where data resides, what controls are in place, and how effectively those controls protect sensitive data
- Enhance controls over access to sensitive data, ensuring proper access to view, modify, and change sensitive data only for the employees who need access to perform their designated job responsibilities
- Repair broken compliance and security processes based on best methods or practices, thereby reducing data loss events and risk
- Improve data classification schemes, enabling a DLP program to more effectively pinpoint the type and location of the data that should be protected

Through thousands of client engagements, CSC has developed proven transition and transformation services to help organizations quickly and efficiently realize the benefits of DLP.

Once a DLP solution has been implemented, CSC has the staff and infrastructure resources to provide 24x7x365 monitoring of information assets, management of technical controls for compliance, enforcement for separation of duties, and experience with real-world business processes for improving the security and availability of IT systems.

Technology: Finally, one of CSC's major strengths comes from its hands-on knowledge and experience with technologies such as Symantec™ Data Loss Prevention Suite, which are essential to an efficient, successful data loss prevention program. Combined with its certified security experts and state-of-the-art infrastructure, CSC offers a comprehensive range of technologies and expertise, including:

- Managed intrusion prevention and detection
- Managed vulnerability assessments
- Technical controls and compliance management tools
- Log assurance and management
- Managed encryption
- Managed antivirus and firewalls
- Identity and access management
- Business continuity and disaster recovery

SEVEN TOP QUESTIONS TO ASK BEFORE YOU EMBARK ON DO-IT-YOURSELF DLP

1. Do you know what data/information is most important to protect?
2. Do you know who's touching that information today?
3. Do you know which channels and vehicles pose the greatest risk of data loss to your particular organization?
4. Do you have robust data governance backed by written policies?
5. Have you chosen the right technology solution(s)?
6. Do you know what to monitor and how to enforce?
7. Do you have executive support and adequate budget to succeed?

CSC contributes at each stage of a DLP solution

CSC has a proven track record offering a full scope of consulting and managed services over many years that help assure success at each step toward achieving an effective and efficient DLP solution. In fact, CSC is currently the only major consulting firm to offer DLP as a managed service. Listed here are the critical stages at which CSC guides its clients from assessment through operation of a complete DLP solution.

DLP Analysis: CSC conducts discovery and risk analysis of data loss potential while helping to identify business requirements and/or challenges as well as establishing priorities and scope.

Strategy/Plan: CSC creates a data classification and policy framework that translates objectives into specific DLP solution requirements to meet business and security priorities. Data classification processes are optimized to work in conjunction with DLP technologies.

Solution Design: CSC customizes a DLP solution according to an organization's specific IT and business environment, including an implementation roadmap that addresses high-priority risks first. CSC then manages the scope and scale of the program to fit requirements and budget.

Implementation/Deployment: CSC introduces initial components of DLP solution in stages, and expands implementation in a coordinated rollout. When managed services are used, CSC handles all infrastructure integration tasks.

Operation: CSC provides comprehensive services to monitor and react to data threats, with a built-in incentive to streamline and enhance DLP processes going forward, optimizing efficiencies and reducing costs.

Continuous Improvement: Over time, CSC develops progressively tighter controls and refines information protection processes and tools as workplace behavior improves and as data management and storage are adapted to maintain an enhanced security posture of the business.

Unique CSC advantages help assure success

In addition to offering the staff expertise and robust infrastructure required for a successful DLP solution, CSC can help facilitate a culture change that increases security awareness and responsibility through employee education combined with managed DLP technologies. Through this education process, CSC and Symantec clients have seen a reduction in their risk of data loss by up to 80 percent compared to existing security programs.

In most cases, CSC can also actively demonstrate ROI for a DLP solution by identifying averted risks every single day if desired, and quantifying those preventive savings or costs avoided in a report for executive management. When evaluating a DLP solution, CSC offers several unique advantages.

KEY TECHNOLOGIES ENCOMPASSED IN A DLP SOLUTION

Monitoring Software

Monitoring software allows organizations to supervise users and detect possible threats to system security in real time. Users that are aware of monitoring software are less likely to intentionally destroy or tamper with data. Any data loss that does occur can be detected, allowing immediate ramification measures to be deployed, minimizing damage.

Data Backup

Regular backups or archives of information should be part of a business continuity program that ensures data can be restored if lost and is stored appropriately to prevent unauthorized access.

Log Files

Log files can provide very detailed information for use in detecting and helping prevent data loss. However, log files can be difficult to analyze or interpret, requiring much time and effort. Log file analysis software should be used to ensure that information is being interpreted and used correctly.

Antivirus Software and Firewalls

Antivirus software and firewalls provide basic protection from hacking and malware, significantly reducing the chance of data being stolen or corrupted.

Physical Security

Providing a secure physical environment for computer systems is essential to prevent theft of the entire system, including data.

- CSC has a proven track record of delivering solutions that produce measurable results, not just a road map or a strategy document.
- CSC is currently the only provider to give your organization the option of implementing DLP as a managed service.
- Because of its long history of leadership in security, business continuity, compliance and information assurance, CSC knows and understands the practical demands of coordinating and operating multiple functions in tandem.
- CSC's in-depth vertical industry experience in government and defense, financial services, healthcare and other fields, brings an added dimension of shared knowledge and insights into more practical, effective DLP solutions.
- By choosing CSC to manage your DLP solution, you gain rapid deployment capability and the flexibility to scale up or down while paying only for what is needed.
- Given its global base of shared resources, CSC offers a DLP solution that provides cost savings from economies of scale within a Security Operations Center environment and infrastructure that is second to none.
- Only CSC can provide you with single-source accountability backed by unique advantages that come from years of real-world experience in security, compliance and data protection. CSC knows how to render pragmatic advice aligned with the risk posture you've chosen for your business.

CSC can assess your data loss risks and help you gain critical visibility into your data flows and usage patterns and how they impact your business governance. Please contact CSC at securitysolutions@csc.com or at one of the regional offices shown below.

Worldwide CSC Headquarters

Europe, Middle East, Africa

Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Asia

139 Cecil Street
#06-00 Cecil House
Singapore 069539
Republic of Singapore
+65.6221.9095

The Americas

3170 Fairview Park Drive
Falls Church, VA 22042
United States
+1.703.875.1000

Australia

26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

References:

- ¹ "Hackers grabbed more than 285M records in 2008," by Jordan Robertson, The Associated Press, April 15, 2009; <http://www.washingtonpost.com/wp-dyn/content/article/2009/04/15/AR2009041500023.html>.
- ² "Data Loss Risks During Downsizing: As Employees Exit, So Does Corporate Data," Ponemon Institute, February 2009.
- ³ "Managing Spend on Information Security and Audit for Better Results," February 2009, IT Policy Compliance Group report, <http://www.itpolicycompliance.com/>.
- ⁴ "7 Requirements for Data Loss Prevention: A guide to evaluating solutions that protect your confidential information assets," by Symantec Corporation, March 2009.