Advisory Services
Security

Data Loss Prevention: Keeping sensitive data out of the wrong hands*

Table of contents

July 2008

The heart of the matter

Data security breaches pose a serious threat. Companies need to reduce risks associated with exposing customer data, losing intellectual property, or violating compliance obligations.

In recent years, an increasing number of high-profile data security breaches have made headlines. These events can not only expose a business to costly and devastating legal ramifications, they also can severely denigrate a brand—sometimes to the point of disrepair.

These breaches don't just happen to the other guy. According to the Global State of Information Security Survey 2007 (GISS), a worldwide study by PricewaterhouseCoopers LLP, CIO magazine, and CSO magazine, more than two-thirds of organizations do not maintain either an accurate inventory of user data or a list of locations and jurisdictions where this information is stored. Only about half of all companies have a policy that addresses the protection, disclosure, and destruction of data. And, although nearly two-thirds of companies worldwide encrypt data in transmission, far fewer appear to encrypt data at rest—in databases (45 percent), file shares (37 percent), laptops (40 percent), and backup tapes (37 percent).

Companies cannot afford to take this lack of data security lightly. Identity theft is rampant, accounting for approximately one-third of consumer complaints received by the Federal Trade Commission during each of the past three years.[1] More than half (54 percent) of identity-theft-related data breaches can be attributed to theft or loss of a computer or electronic transportable media[2]—a percentage unlikely to diminish.

State and federal regulators who are concerned about the protection of sensitive data are starting to impose stronger controls. They are levying stiff civil and financial penalties against organizations and their top executives for failure to comply with regulations, and are requiring that companies send security breach notifications to affected parties. Trial by fire has shown some organizations that noncompliance-related expenses can be astronomical. In 2007, the average loss from a data breach was $6.3 million, an increase of 31 percent from 2006.[3]

Complying with government regulation and securing sensitive information across the data life cycle can be challenging as well as costly. With third-party outsourcing skyrocketing during the past several years, some companies are having difficulty keeping track of the data leaving their network. Others are finding it hard to ensure the integrity of data once it reaches its intended location. GISS shows that only one-quarter of companies believe they have an accurate inventory of third parties using customer data. And only one-fifth of those are confident in their outsourced vendor's security.

With consumers and regulators demanding more control over sensitive data than ever, it is clear that—whether you're a security leader or a business line executive—now is the time for you to start better protecting your company's customer data, core intellectual property, trade secrets, and regulated data.

1 Federal Trade Commission. 2008. "Consumer Fraud and Identity Theft Complaint Data": 4
2 Ponemon Institute LLC. 2007. "Ponemon Study Shows Data Breach Costs Continue to Rise": 1-2
3 Symantec. 2008. "Trends for July - December 07". Symantec Global Internet Security Threat Report Volume XIII: 12-16

Is it possible that your company might experience a costly data breach? You should be concerned if:

- Your company is about to implement a workforce reduction. Is it possible that affected employees might take customer account lists, financial data, or strategic plans when they leave? Proprietary information could end up in the hands of your biggest competitors or be widely disseminated online.
- Your company is using an outside vendor to print customer mailings, and the unencrypted, nightly file transfer contains excessive and potentially sensitive customer data. Could your vendor be improperly using the data or improperly securing the data? If so, your customers' identities could be at risk.
- Employees throughout your company regularly export data from the customer relationship management system and send it, typically unencrypted, to their personal e-mail addresses so they can work from home. Your data may be compromised on someone's home computer.
- You don't know where your most sensitive data resides across your enterprise, and you may not have the appropriate controls in place to prevent unauthorized access. You could be in violation of local or federal regulations as well as non-compliant with your company policies.

By aligning a well-designed Data Loss Prevention program with an overall data protection strategy, you can gain control over sensitive data, reduce the cost of data breaches and achieve greater visibility into how data are used throughout your organization.

An in-depth discussion

Point solutions don’t work. For data loss prevention (DLP) to be effective, companies must decide on the right strategy, engage the right people, target the right data, and employ the right technology.

Organizations need to understand what controls are in place to protect sensitive data

As most companies move toward deploying a DLP solution, they often realize that they could be getting more out of their existing controls. Many companies see that their disparate point solutions, which do not interoperate, are preventing them from achieving a maximum level of protection.

At PwC, we believe there are four key components to any successful DLP program. They include:

1. Strategy—Decide on the desired result, develop a plan, and monitor progress

Align DLP programs with overall data protection strategy. Your detailed data protection strategy should incorporate various controls and protective measures at different points across the data life cycle. These include collection, use, transit, storage, archival, and destruction. Use DLP, which is a vital component of this overall strategy, in conjunction with other protection technologies, such as encryption, persistent protection, and file destruction.

Look for leaders, not silver bullets. It is important that you carefully consider and thoroughly evaluate potential DLP vendors. Well-qualified vendors offer comprehensive solutions with centralized workflow capabilities, integrated policies, and customized reporting. They also are able to provide you with a modular DLP program that offers capabilities across three main vectors: data at rest, data in motion, and data at endpoints.

Obtain stakeholder buy-in across the organization. While deploying your DLP solution, be sure to involve the stakeholders from the beginning. This ensures that the parties fully understand the business requirements and the impact they may have on operations, employee behavior, and corporate culture. At a minimum, stakeholders include representatives from the following groups: privacy, IT, security, investigations, human resources, legal, compliance, audit, and the lines of business.

Align key performance indicators (KPIs) with your overall data protection strategy. Linking performance and operational KPIs to your DLP strategy allows you to more effectively measure your organization's performance, which ultimately enables you to make more informed business decisions. Commonly used KPIs include: number of data leakage incidents, percentage of network coverage, and percentage of application coverage. To make this process as seamless as possible, you should eliminate analysis and reporting activities that are not directly aligned with the KPIs or DLP strategy.

2. People—Increase resource effectiveness

Assign roles and responsibilities. A detailed responsible, accountable, consulted, informed (RACI) matrix and staffing model helps you determine how the various functional areas within your organization factor into the planning, design, implementation, and operation of the DLP solution. Additionally, a RACI clearly defines each stakeholder's role and helps facilitate stakeholder buy-in.

Understand organizational culture. Depending on the vendor, end users may consider DLP products intrusive. A sound understanding of organizational culture helps you establish which features are important to your organization and how much impact users are willing to bear. This should help you achieve a smooth, complete, and successful implementation.

Identify data owners. Data owners understand the importance of their data in relation to the business and should be the primary decision makers involved in remediation efforts. You should immediately identify the data owners; establish relationships with them; and engage them in effective, ongoing, two-way communications.

3. Process—Streamline, simplify, and standardize processes through the data life cycle

Establish a data classification schema. When considering a DLP program, the first and most important step is to identify sensitive data and assign a classification. This process helps you create the DLP policies and rules you need to detect and respond to incidents that involve sensitive data. It also allows you to better understand what data your organization considers important and how that data should be protected.

Conduct a data protection assessment. Analyzing the existing technology and process controls helps you identify control gaps. Base your data protection assessment on an established risk management framework and detailed classification scheme. Make certain that you encompass all areas of the organization, catalog the location of sensitive data, estimate the amount of exposure the organization faces, and measure the potential magnitude of the loss of sensitive data.

Perform privacy impact analysis. Take particular care when deploying any technology you use to actively monitor and store employee communications that may be personal. A detailed privacy impact analysis enables you to identify potential concerns regarding the use of DLP technology. It also helps you understand the requirements for deploying the technology, and protects the sensitive data captured by the technology. A privacy impact analysis is especially important for organizations with operations that extend across various countries and privacy laws.

Develop enabling business processes. It is virtually impossible for technology to be effectively or efficiently deployed in isolation. For your program to be successful, it is essential that you consider the various business processes that support the use of DLP technology—event management, event classification, business unit remediation, incident response, reporting, and system operations.

4. Technology—Use technology solutions to detect and prevent data loss

Deploying solutions typically occurs modularly. In working with hundreds of clients on data protection issues over the past few years, we've seen a consistent theme: companies want to deploy modular solutions that provide the greatest coverage with the least amount of internal disruption. This approach makes it possible for you to seamlessly implement more robust data protection solutions down the line as technologies mature and your business needs dictate.

Data loss prevention control points span the environment. DLP technologies are designed to address three distinct scenarios: data at rest, data in motion, and data at the endpoint. Protection techniques aimed at each of these scenarios offer distinct benefits and mitigate different types of risk.

» **Data at rest** typically resides within stationary repositories, such as file systems, databases, desktops, and groupware. Common risks associated with this type of data include the lack of visibility into where sensitive data is stored, the lack of understanding around who has access to the sensitive data, and the lack of secure storage for sensitive data to prevent theft and loss. Using DLP products to address these issues allows you to reduce the proliferation of sensitive data and enables you to drastically improve data protection controls.

» **Data in motion** consists of information that is electronically transmitted outside an organization's network via e-mail, online chat rooms, and other methods. Common risks associated with this type of data include the loss of sensitive data through various communication mediums, the harvesting of sensitive data by malware, and broken business processes that expose sensitive data. With DLP products, you can stop sensitive data loss through electronic means, and enforce compliance with local and federal regulations, as well as corporate standards and policies. You can also identify broken business processes.

» **Data at the endpoint** relates to information stored on laptops and portable storage devices. Stolen laptops and portable storage devices provide unauthorized individuals with portals into your data storage and transport endpoints, and give them immediate access to "offline" data. DLP products help protect sensitive data even when equipment is offline by identifying sensitive data stored on portable storage devices and restricting use of those devices.

Walk, don't run to prevention. Many vendors offer a prevention component that gives you the ability to block or prevent sensitive data from leaving your organization. These products are still maturing and, in their current state, using them to prevent or block data could disrupt critical business processes and negatively impact your business operations. Your detailed implementation plan should address the pros and cons of deploying technology with prevention or blocking capabilities.

Continuously tune policies. DLP is not a "set it and forget it" type of technology. As you move forward and see what works and what doesn't, you can refine your polices to be more accurate. Our experiences show that organizations that take a deliberate and iterative approach to DLP programs realize benefits more rapidly, because they involve the appropriate stakeholders, execute due diligence, and reduce impact due to proactive communication throughout the implementation process.

What this means for your business

An effective solution provides transparency over data use, controls sensitive data, and reduces the likelihood and costs of a data breach.

You can increase customer confidence and reduce risk with a strong data loss prevention strategy

More and more, organizations are developing enterprise-wide approaches to governance, risk, and compliance. They create unified control sets that allow them to more easily demonstrate compliance to a myriad regulations. Establishing unified procedures for gathering and documenting data reduces the need to ask the same questions of the same people. DLP solutions play an integral part in determining where data truly is and, thus, where companies need to position resources to conform to their chosen approach.

A well-architected DLP program can help you:

- Improve data classification schemes. With a DLP program, you can more effectively pinpoint the type and location of the data you want to protect.
- Gain an understanding of the data life cycle. An effective DLP program includes a complete data flow and gap analysis, which helps you understand where data resides, what controls are in place, and how effectively those controls are protecting sensitive data.
- Enhance controls over access to sensitive data. Your DLP program must allow you to limit access to view, modify, and change sensitive data to the employees who need access to perform their normal job responsibilities.
- Repair broken business processes. A well-thought-out DLP program enables you to fix the broken business processes that put your company at risk, and ultimately reduce data loss events.

How PwC Can Help

PwC provides a thorough end-to-end privacy service that helps you assess your current environment and subsequently plan, manage, and implement a successful data protection program. Our proven methodology is specifically targeted to help you identify and address each facet of an effective, efficient, and sustainable DLP program.

Risk Assessment

We conduct a technical evaluation showing the actual unprotected data leaving the enterprise on the wire, the uncontrolled data in repositories or file shares, and unencrypted data on removable media, redacted to protect identity information and other sensitive data prior to review by privacy practitioners.

Enterprise Privacy Framework Development

We analyze your privacy requirements from relevant local and international regulations and develop a privacy framework addressing the regulatory requirements. We also recommend technologies that help you implement the framework within your organization.

Data Loss Prevention (DLP) Technology Deployment

We help you evaluate the DLP technologies and deploy the selected DLP solutions in your network. With the right DLP solution, you can reduce risks of data loss or leakage by insiders and inappropriate transfer of critical and sensitive information.

Data Classification and Ownership

We help you develop the application inventory to identify the critical information assets and their owners. We also work with you to develop a classification scheme that prescribes certain levels of controls, depending upon the classification of the information, to help facilitate proper handling of data based on the sensitivity level.

Business Process Creation

We create content-monitoring operational practices that integrate with the selected data loss prevention technology. By helping you create a realistic and well-managed DLP program, PwC can help your company build reliable controls around access to your data at rest, in motion, and at the endpoint, and help ensure that your company name does not appear in the next headline about a data security breach.

www.pwc.com/security

To have a deeper conversation on the industry or on any of the topics mentioned, please contact:

Gary Loveland
Principal, National Security Leader
gary.loveland@us.pwc.com

Brad Bauch
Principal, Houston
brad.bauch@us.pwc.com

Rik Boren
Partner, St. Louis
rik.boren@us.pwc.com

Michael Compton
Principal, Detroit
michael.d.compton@us.pwc.com

Scott Evoy
Principal, Boston
scott.evoy@us.pwc.com

Kurt Gilman
Principal, New York
kurt.gilman@us.pwc.com

Joe Greene
Principal, Minneapolis
joe.greene@us.pwc.com

John Hunt
Principal, Washington
john.d.hunt@us.pwc.com

Jerry Lewis
Principal, Dallas
jerry.w.lewis@us.pwc.com

Mark Lobel
Principal, New York
mark.a.lobel@us.pwc.com

Sloane Menkes
Principal, Washington
sloane.menkes@us.pwc.com

Joe Nocera
Principal, Chicago
joseph.nocera@us.pwc.com

Chris O'Hara
Principal, San Jose
christopher.ohara@us.pwc.com

Fred Rica
Principal, New York
frederick.j.rica@us.pwc.com

Andy Toner
Principal, New York
andrew.toner@us.pwc.com

This publication is printed on Mohawk Options PC. It is a Forest Stewardship Council (FSC) certified stock using 100% post-consumer waste (PCW) fiber and manufactured with renewable, non-polluting, wind-generated electricity.