



Data Loss Prevention

In today's always-connected, increasingly mobile world, the threat of losing confidential data to malicious attacks, accidents or negligence is greater than ever. However, with advanced technology solutions, organizations can minimize risk by identifying and monitoring their critical data and putting in safeguards to protect it from loss or misuse.

Table of Contents

- 1 Executive Summary
- 2 The Risks of Data Loss
- 3 Assessing the Threats
- 4 Identifying the Data
- 4 Protecting the Data
- 5 Going Beyond Monitoring
- 6 Best Practices for Setting DLP Policies
- 6 The Biggest Risk of All: Not Taking Action
- 6 Partnering with CDW

Executive Summary

IT professionals are under increasing pressure to protect their organizations from the loss of critical data. With businesses becoming increasingly mobile and connected, it is more challenging than ever to secure data against both malicious attacks and accidental loss resulting from lack of policy, enforcement or education. In addition, those who maliciously steal data have become more sophisticated and organized in their use of technology.

The stakes are huge: Lost data can severely damage a company's reputation, result in significant financial losses — including fines levied by state or federal governments — and harm the overall business in any number of ways, from lost customers and revenue to the theft of valuable intellectual property.

However, while the threats have become more sophisticated, so has the technology to prevent the damage inflicted by data loss and theft. Many innovative organizations are turning to data loss prevention (DLP) solutions as a way to avert and, in some cases, intercept the threats that can result in critical data loss.

In this white paper, we address the risks of data loss and how they can impact an organization from a business, financial and regulatory perspective. We also discuss the importance of assessing threats and the need for business leaders and decision-makers to be aware of vulnerabilities. We then look at the ways in which organizations can use DLP technologies and policies to create an overall strategy to identify and protect data, prevent breaches and minimize the chance of losing sensitive information. This includes a discussion about best practices for setting DLP policies and why you should consider solutions that go further than simply identifying and monitoring data. We also examine the biggest risk of all: the risk of doing nothing. Finally, we outline how an organization can go about building a comprehensive DLP strategy.

The Risks of Data Loss

Data is the lifeblood of any organization. The digital bits and bytes that are stored in our systems and sent across our communications links represent sales, customer, personnel and personal information, as well as information about illnesses, lawsuits, corporate strategies, corporate takeovers, customer preferences, pricing, patents and branding plans. In short, anything and everything that has to do with a business, its customers and its employees is in digital format somewhere in the corporate IT infrastructure. Not only is confidential data all over the place, it is growing all the time and is often being created and transferred at a wide range of endpoints using an ever-expanding range of user devices. Typically, data creators, owners and users are not IT staff and, unfortunately, not well trained in managing security.

Failing to protect such data from theft, leakage or any other type of disclosure has the potential of exposing an organization to dangerous, expensive and possibly crippling after-effects. What are the risks corporate leaders should be considering when evaluating the potential impact of breaches and data loss?

1. **Financial.** Is it even possible to measure the damage to an organization's reputation and possible harm to its customer base? People steal data because it is worth money. A customer's name and Social Security number can be used to obtain a loan, and there is a booming black market for functional credit card numbers. Information is stolen for its financial value — for an organization, this can mean financial loss, lost business, lost customers and negative media coverage.
2. **Regulatory.** Forty-five states have enacted legislation requiring notification of security breaches involving personal information.¹ In the state of Michigan, for example, organizations can be fined \$250 for each failure to provide notice and for each record not deleted. A single data security incident can cost as much as \$750,000 in fines. In the U.S., data brokerage firm ChoicePoint Inc. was fined \$15 million by the Federal Trade Commission after a data breach exposed information about 163,000 consumers to an alleged crime ring. Since many businesses now operate globally, organizations should be aware that other countries are also cracking down on data loss. In the UK, laws were recently enacted that enable the information commissioner to fine organizations up to a half-million pounds for a breach of the Data Protection Act. In 2008, Zurich Insurance's UK branch was fined more than 2 million pounds for losing the information of 46,000 customers.
3. **Business.** When data is lost or stolen, a business can suffer from not having that information and from having land in the hands of a competitor. Think of a salesperson with an account list or an automobile manufacturer that has detailed drawings of its next-generation fuel-efficient engine, or a company embarking on a rebranding or marketing campaign. There is a huge risk in not having such critical information, and an even greater risk of having that information fall into the wrong hands.

Where Are You Vulnerable? Let Us Count the Ways

DataLossDB (www.datalossdb.org) is part of the Open Security Foundation, a nonprofit organization funded and operated by information and security enthusiasts. The DataLoss database is a free and open resource for the collection and dissemination of data loss incident-related information.

To get a sense of just how and where organizations are vulnerable, we looked at a recent two-week period on the database. In that time, 20 separate incidents of data loss involving more than 200,000 individual records were reported. What's more, those incidents of data loss resulted from a wide range of causes, from malicious attacks and fraud to accidents and lost media. Here are a few of the incidents, as characterized by DataLossDB:

Remember these all happened in just a single two-week period, chosen at random:

Web: 150,000 names, addresses, genders, e-mail addresses and customer profiles posted on the Internet by provider. Source: *Inside Accidental*

Stolen Laptop: 8,300 names, Social Security numbers and some drivers' licenses stolen from laptop in rental car. Source: *Outside*

Virus: 300 credit card numbers stolen via virus from restaurant. Source: *Unknown*

E-mail: E-mail containing employee Social Security numbers inadvertently sent to 144 (wrong) addresses. Source: *Inside Accidental*

Hack: 200 patients' information exposed due to former employee's password used to access medical records. Source: *Outside*

Fraud: 17,000 patients' medical records accessed by employee. Source: *Inside Malicious*

E-mail: 4,000 employee names, addresses, birth dates, Social Security numbers and salaries sent by inadvertent e-mail. Source: *Inside Accidental*

¹Regulations and Compliance: The Business Justification for Data Security, ZDNet, January 20, 2010

4. **Reputation.** Perhaps the biggest risk of data loss is the potential damage to the company's reputation. Companies that have suffered from high-profile breaches, such as TD Ameritrade, have lost significant numbers of customers and have faced class-action lawsuits that further damage their reputation. With the Internet, every news story is saved forever, making it almost impossible to escape the publicity of a major breach no matter when it occurred. Here's what the Online Trust Alliance, a non-profit organization addressing online trust and abuse, says about reputational risk:

"Few if any other events or incidents can damage a company's reputation and consumers' trust more than a breach of personal, sensitive or corporate data, which impacts not only a company's customers but also their partners, stockholders and employees. High-profile breaches risk scrutiny from consumer advocates and regulators, not to mention fines and loss of business resulting in negative impact to stockholder value."

The threats of lost and stolen data are real and potentially devastating. According to the Theft Research Center, data breaches involving personally identifiable information increased by more than 600 percent between 2008 and 2009, with more than 222 million records being compromised.² A study by the Ponemon Institute estimates that the average cost of a data breach is more than \$200 per customer record. The average cost of a data breach to a company is \$6.65 million, and that does not include some of the "softer" costs involved in unresolved lawsuits or the impact of reputational damage. In the same survey, 84 percent of respondents expressed increased concern or anxiety about the loss of data, and 62 percent indicated that they had been notified at one time or another that confidential data had been lost or stolen.³

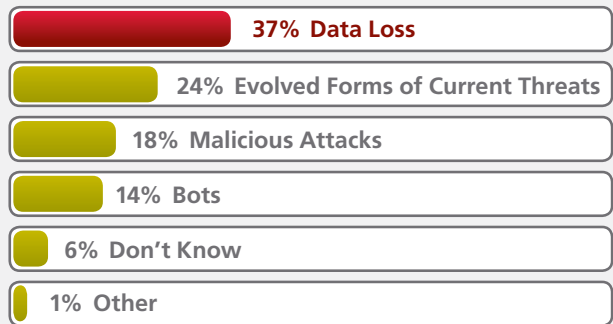
Assessing the Threats

One of the challenges in trying to assess and mitigate the risks of data loss is that the threats are fairly ubiquitous. With an increasing number of devices attached to the corporate network, there are more opportunities for intruders to gain access and for data to escape, either through malicious intent or through negligence, or carelessness or by accident. In addition, changes in the way individuals use technology can create new threats: Innovations such as cloud computing and social networking, for example, are increasing risk and forcing business and IT professionals to address ever-changing vulnerabilities to corporate data. In one nine-month period two years ago, the number of websites carrying malware

increased from 1,068 new sites discovered per day to 5,424 per day, an increase of more than 400 percent, according to research firm Osterman Research Inc.⁴ In a 2010 study by CDW, IT security decision-makers identified data loss as the next big cybersecurity threat (see chart).⁵

The Next Big Threat

Question to IT Security Decision-makers:
What is the next big cybersecurity threat your organization will face?



In developing a plan to assess and address the problem of data loss, it is critical that business leaders understand the threats, and articulate and measure just how damaging those threats could be to the overall organization. Malicious theft of data is a huge threat to business, and if your company is targeted, it can mean significant financial losses and penalties, as well as major damage to your brand. Even if your organization is not a target, there are an almost infinite number of ways that information deemed valuable, critical and private can be leaked from the company.

Part of the challenge for IT departments is to understand the threats and their potential impact — not just to stop them from happening, but to make sure that the business executives who own the data and operations realize just how vulnerable the business may be. What are some of the factors that will motivate the business decision-maker? Here are a few: awareness of a breach at another company and the financial havoc it may have caused; a new regulation that could result in penalties for noncompliance; or, most effectively, awareness that the organization itself is vulnerable to multiple breaches at multiple locations.

For these reasons, any major DLP strategy should start with a risk assessment. This is a crucial step in forging the necessary awareness at the executive level to earn the sponsorship and support to complete a successful project and alter the busi-

²Data Breach & Incident Readiness Planning Guide, Online Trust Alliance, January 2010

³Fourth Annual U.S. Cost of Data Breach Study, Ponemon Institute, January 2009

⁴Protecting Your Network Against the Growing Danger of Web Attacks, Osterman Research, Inc., ©2009

⁵CDW 2010 Threat Prevention Straw Poll Report

ness processes that put data at risk. This means determining what data is most critical to the business — that is, the data it can least afford to lose — and assessing where that data lives, how it moves and its risk of exposure. At this point, it is important to work with an expert and experienced third-party team, such as CDW, that is not tied in to any particular vendor or solution and can offer a range of options based on the specific needs of the business.

Indeed, individual businesses will find that the assessment process and vulnerabilities it exposes are unique, based on a wide range of factors. The assessment enables each company to get a snapshot of what's happening in its own environment and to focus on the impact of vulnerabilities so that the corporate or executive sponsor understands both the risk of data loss — exposing the vulnerabilities — and the damage that such a loss could incur. Some assessments, for example, can involve a three-week analysis of what has already happened within the network.

When this analysis is done, business decision-makers often learn of something that absolutely appalls them. For example, an automated process exported 10,000 records a day — in clear text. Even in organizations where there are established policies to prevent data loss, an assessment usually uncovers numerous instances of users breaking the policy and exposing the organization to potential breaches. A solid assessment conducted in partnership with a knowledgeable third party helps organizations understand exactly where their “crown jewels” are and where they are going, and will give decision-makers the data necessary to understand and manage the risk that exposure represents to the business.

Identifying the Data

The assessment will determine where your confidential data is located, how it is being used and the risks the organization is accepting — unknowingly — on a daily basis as a result of its current business and user practices. Once the assessment process is completed, business leaders should be ready to undertake a serious DLP strategy.

The next step is to work with your third-party partner to refine existing data security policies so that they more appropriately define confidential data and how it can be used. The goal is to align these refinements with the executive leadership's response to the risk assessment. Once the appropriate data security policy is created, the next step is to select a DLP vendor that can translate the policy into technology and help the organization utilize that technology to gather real-time and comprehensive information on policy compliance.

Most vendors of DLP technologies offer some sort of analysis engine that can identify the data. An analysis engine can look at an open e-mail attachment, for example, and determine that the contents contain a Microsoft Word document that includes the results of confidential research. It can do this by looking at the content and the data itself, and it can analyze the data while it is in motion — for example, in e-mail, file transfers and instant messages or as web traffic. It can watch the edges of the network and prevent an e-mail message from leaving the network if it contains any information that the company has deemed confidential, and also prevent messages from entering the corporate network if they pose a threat.

An analysis engine should also be able to identify and view data at rest. In any corporate network, a directory tree can contain millions of files, some of which haven't been looked at in years. This can be a massive amount of data, and it is almost guaranteed that within these forests of files, there will be some highly confidential data. What if there was a document buried somewhere in the database with 500,000 Social Security numbers that could be accessed easily by a temporary receptionist? That happens more often than most people would like to know. If you have DLP technology in place, it is trivial to identify and contain that data, preventing it from being accidentally or maliciously removed from the database. DLP solutions should be able to identify confidential data within databases and e-mail repositories, and on all types of devices, including servers, desktop computers, laptops and smartphones.

Protecting the Data

Once you have the engine in place to identify the data and determine where it is at risk, the next question you have to ask is, “What are we going to do about it?” You can see the risks, but how do you stop them? And, assuming you want to eliminate the risks, how much are you willing to pay? This becomes a matter of setting business priorities and policies, and then addressing those problems with the technology.

The primary goal of the technology is to dynamically identify and find the data. In terms of protecting the data, a tremendous amount of work has to be done to determine where it sits, where it moves and where it is at risk. This process also includes a substantial investment in time and resources to educate people in the organization about how to work securely. The second step in this methodology is the monitoring of confidential data, also called remediation, which is making sure that users are educated and policies have been reinforced. At this point, you need to take a snapshot of your

environment and determine which business processes need to be changed or fixed.

By solving existing problems and cleaning up inadequate or poorly enforced policies, you should be able to substantially reduce the number of data security incidents and move on to the third step, which is notification and education. This is where you start implementing the new policies along with the new technologies. For example, you can automatically encrypt certain e-mail that might contain confidential data, or you might not allow it to be saved on a laptop or prevent it from being sent. At this stage, you can also work with users on where and when they may be at risk for violating policies and increasing the risk of breaches — and you can educate them on how to handle data correctly. At the next stage, which is prevention, you flip the switch and let the technology do what it needs to do to prevent data loss. If you decide that confidential data should never leave the organization, for example, the technology is in place to ensure that. The methodology is outlined in the figure below.

Going Beyond Monitoring

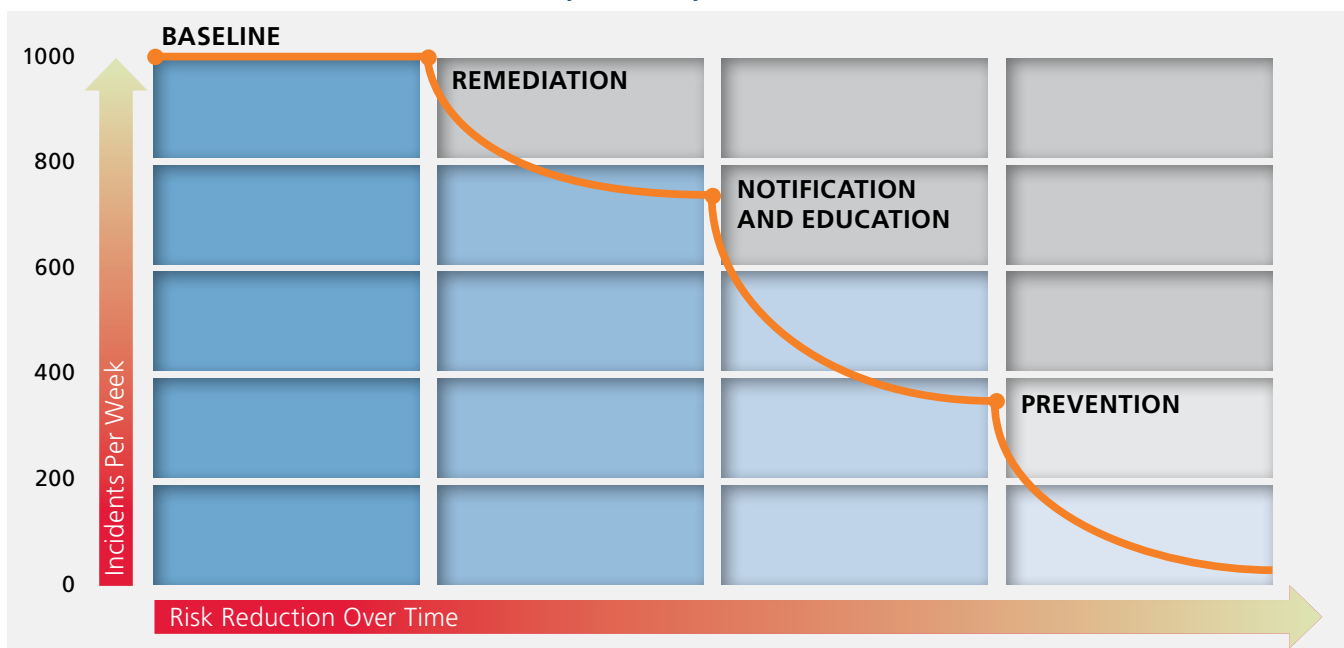
Within the DLP market, there is a variety of technological solutions. All of the leading vendors offer some sort of monitoring platform that identifies key data and where and when it may be vulnerable. For most, monitoring is as far as the organization is willing to go. With monitoring, they at least feel comfortable that they have identified their critical data

and can determine where, when and how it is at risk and then take the steps necessary to plug up the leaks.

However, while data monitoring is absolutely crucial and the foundation of any major DLP initiative, there are some risks involved in doing only data monitoring. For one, data monitoring usually addresses only data in motion. So, for example, the situation with the temporary receptionist who has access to 500,000 Social Security numbers could be a risk with a monitoring-only solution. Without a prevention configuration in place, it is difficult to prevent a breach from happening. In reality, most organizations start with monitoring and then add incremental prevention features either over time or in direct response to an incident. This is not always the best solution, however, because it doesn't necessarily fix the problems and it often forces the IT organization to go back to the CEO or CFO to get additional funding.

For organizations that are ready to go beyond monitoring, the next steps are to add prevention, resolution and encryption technologies and to implement the proper policies, education and changes to business processes. Again, having a strategic business partner here is critical, because writing clear, concise and enforceable policy is just as important as choosing the right vendor and the right technology. As you get deeper into building a comprehensive plan and strategy for DLP, technology is available to build a fairly ubiquitous solution, enabling the organization to identify confidential data in a wide variety of media and formats, including e-mail,

Measurable Risk Reduction — DLP Project Lifestyle



instant messages, web traffic, data stored on local or USB drives, and even data sent to a printer or fax machine. In addition, a DLP solution should be able to identify policy violations and proactively block confidential data from leaving the network at any point, whether it is through the corporate network or database or through any endpoint device.

Best Practices for Setting DLP Policies

In developing a successful DLP strategy, it is important to choose the right technology solution and equally critical to establish policies that are easily understood, clearly articulated and consistently enforced. Here are some of the best practices in setting policies for a successful DLP deployment:

1. **Make the Policy Appropriate:** The policy should be written by the data owners as opposed to the technical security people. Technologists can get mired in the details, while the data owners have a better understanding of which data represents the organization's crown jewels. Security and DLP policies must have a bearing on reality and focus on what is truly important. Most people have a low tolerance for policy in general, so it is important to get their buy-in. It is one thing to have someone in IT security tell a user, "You can't do this." It's quite a bit more powerful if the executive of the business unit says, "If you're going to be touching XYZ information, you will work with it in this way — and you're NOT keeping it on your laptop! All copies are to remain in this secure central location!"
2. **Make the Policy Simple:** Many organizations tend to write their policies based on those of other organizations or they look on the Internet for standards. This adds steps, tends to make the process more convoluted and often ends up in a policy that is stuffed with rules that are not appropriate or even applicable. Write your own policy, make it clear and concise, and get input from all of the people it will impact.
3. **Make Sure the Policy Suits the Business:** You don't want to implement security policies that are detrimental to productivity or business success. For example, you may have a policy that prevents HR data from being transmitted outside of your organization. But what about the benefits person who has to send information on new employees to a healthcare provider? You have to give that person a secure way to do his/her job. In reality, if you make it too hard, employees will send an e-mail anyway or, even worse, take the information home and send it

from their personal e-mail account. This is why an assessment is so critical: It allows the organization to fix broken business processes in a way that makes it possible for individuals to conduct business securely.

The Biggest Risk of All: Not Taking Action

Here is an extremely important point to consider: Just because you are not aware of the risks does not mean that they aren't there and your organization is not vulnerable. Implementing a successful DLP solution often comes down to arguing for awareness versus ignorance and making the case that, for the first time, DLP technology is giving IT and business professionals a critical tool in protecting their organizations from the threat of all types of data loss, malicious or otherwise.

The growth in the number of devices attached to the network and the increasingly mobile nature of users has meant that IT departments have been getting less and less visibility into the type of information that is leaving and entering the organization, and less control over what users are doing with their devices. DLP technology is a way for IT organizations to regain control without having to place severe limitations on users and without having to do anything that would compromise the ability of the business to conduct its normal operations.

Incidents that the IT department would have had no ability to even identify in the past can now be addressed — in advance — through the use of state-of-the-art technology. Here's a real-world example: A large hospital where a small department was working with an independent laboratory. On a routine basis, the department would send e-mails to the lab, either assuming that the link was secure or not even thinking about whether security was an issue. The IT department didn't even know there was a link between the two organizations and that there was any communication at all being sent. With DLP technology and the proper rules and procedures in place, those e-mails were identified and monitored, and the organization was empowered to alter that business process to appropriately secure the exchange of confidential information.

Partnering with CDW

In evaluating, understanding and addressing the threat of data loss within your organization, it is critical to work with a third-party organization that is experienced in both assessing and mitigating risk. CDW's highly trained and certified security engineers understand your complete IT environment and business aims. They can deliver security solutions that

seamlessly integrate with your systems to minimize risk to the greatest possible degree.

In addition, CDW has thorough knowledge of all relevant federal, state and industry standards and regulations, including:

- Payment Card Industry (PCI)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Gramm-Leach-Bliley Act (GLBA)
- The Sarbanes-Oxley Act (SOX)

CDW knows that the successful achievement of your business goals depends on properly safeguarding your IT environment and data assets. CDW also understands that good security is a careful balance between confidentiality, integrity and availability. In choosing the right partner, it is important to remember that there are thousands of ways your organization can be exposed to losing data, and far fewer ways to successfully protect it.

By partnering with CDW, you can minimize the risks substantially, while protecting your organization from the financial, regulatory and business challenges that come with the loss or theft of confidential data. CDW will work with you on your risk assessment so that the decision-makers in your organization will be able to see the magnitude and severity of the problem. CDW will then help you define the scope, budget and support required to implement a successful solution.

To see if you qualify for a risk assessment, please contact your CDW field account executive or **visit cdw.com/dataloss for more information.**

About CDW

CDW is a leading provider of technology solutions for business, government, healthcare and education. Ranked No. 41 on *Forbes'* list of America's Largest Private Companies, CDW features dedicated account managers who help customers choose the right technology products and services to meet their needs. The company's technology specialists offer expertise in designing customized solutions, while its technology engineers and solution architects can assist customers with the implementation and long-term management of those solutions. Areas of focus include notebooks, desktops, printers, servers and storage, unified communications, security, wireless, power and cooling, networking, software licensing and mobility solutions.

CDW was founded in 1984 and as of March 31, 2010, employed approximately 6,150 coworkers. In the 12 months trailing March 31, 2010, the company generated sales of \$7.6 billion. Intently focused on responding to customers' technology needs with a sense of urgency, CDW helps customers achieve their goals by providing the right technology products and services they need — when they need them.