

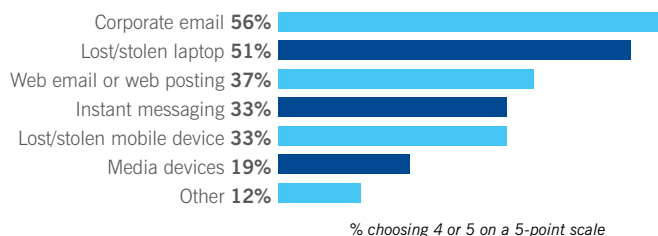
Stopping data leakage: Making the most of your security budget

Organizations are increasingly aware of the acute need to control the information that flows into, through and out of their networks. This paper demonstrates the need for a high-profile acceptable use policy to prevent data leakage, gives practical guidance on how to use your security budget effectively to protect data at the gateway and endpoint, and highlights the benefits of encryption in securing data in the event that it does get stolen or lost.

Stopping data leakage: Making the most of your security budget

After years of battling intrusions, viruses, and spam, organizations now find themselves wrestling with a relatively new but hugely significant security issue: data leakage. By March 2008, the inadvertent exposure of company confidential information was already being cited by analyst IDC as the number one threat, above viruses, Trojans, and worms¹. At the end of the year, 80 percent of respondents in another survey agreed that data security was one of the biggest challenges facing them, with 50 percent of respondents admitting they'd experienced a data leakage incident in 2008.²

IDC's survey identified intellectual property as the most common type of information leaked and 81 percent of respondents saw information protection and control (IPC) – defined as monitoring, encrypting, filtering, and blocking sensitive information contained in data at rest, data in motion, and data in use – as an important part of their overall data protection strategy. The highest priority IPC solution was data leakage prevention (DLP) deployed at the organization's perimeter and on endpoint computers.¹



Importance of monitoring employee use¹

The intentional or accidental exposure of information, ranging from legally protected personal information to intellectual property and trade secrets, is something that affects the IT environment in its widest sense, involving lost or stolen laptops, USB keys and other devices, email, and Web 2.0 applications, such as IM. Respondents to IDC's survey demonstrate just how many points of exit there are (see figure 1).

The challenge now is not simply to protect data from the threat of theft or corruption from malware, but to add a second security layer preventing data being accessed if it is lost.

The growing importance of DLP

There are several reasons for the movement of data leakage prevention to the forefront of enterprise security.

High-profile, reputation-damaging data leaks

Bad publicity from data leakage can result in damaged reputation, lost customers, and sometimes even ruin for companies.

The number of well-publicized examples of data security breaches is growing significantly. Government bodies, financial organizations, education institutions, industry giants and even presidential candidates – no-one is immune. Recent high-profile incidents have included:

- Secret government documents on al Qaeda and Iraq were left on a commuter train in the UK. (Jun 2008)³
- The personal information of almost 1000 bank customers was lost by an employee of Bank of Ireland, after the data was copied onto an unencrypted USB memory stick which was then lost. (November 2008)⁴

- An email containing names, positions, salaries, and social security numbers of 192 faculty and staff members was accidentally sent to Ohio State University Agricultural Technical Institute students. (May 2008)⁵
- Hackers were charged with stealing more than 40 million credit and debit card numbers from nine US retail outlets by breaking into the wireless networks of major retailers. (September 2008)⁶
- An investigative reporter for MyFoxDC bought a Blackberry device during the McCain-Palin US presidential campaign's sale of its used office inventory, only to find 50 phone numbers for people connected with the campaign and hundreds of emails. (December 2008)⁷

Regulations

Government legislation

Governments worldwide have introduced increasingly stringent data protection legislation, such as the US's Sarbanes-Oxley Act, HIPAA, and Gramm-Leach-Bliley Act, and the UK's Data Protection Act, to provide suitable controls over sensitive company information. Organizations found to be in breach of the legislation can be fined and forced to put solutions in place to prevent a recurrence. The California Senate Bill 1386, introduced in 2003, was the first to require that organizations notify all affected individuals if their confidential or personal data has been lost, stolen, or compromised. This public disclosure is now required by 35 states. Many regulations also require regular audits, which an organization may not pass if the right controls are not in place.



Today, protection must focus on controlling access to the information, not on blocking the perimeter.



PCI DSS

Alongside government legislation sits PCI DSS (Payment Card Industry Data Security Standard). Created by multinational corporations, it is enforced on merchants as a part of their terms of being allowed to accept credit card transactions. Organizations that cannot demonstrate PCI-compliance at an audit are subject to sanction even if no actual data leak has occurred. PCI's reach across international boundaries and its ability to respond quickly to change – it last extended its scope in October 2008 – makes it as important a security standard as any local or national legislation.

Cost

In addition to legal costs, organizations have to deal with the less tangible costs of recovery and commercial fallout, such as lost business, or withdrawal of credit card merchant status. All these costs have been rising steadily.

Cost of a data breach

- » Up 11 percent since 2006
- » Average cost per breach – \$6.6 million
- » Average cost per record – \$202
 - for healthcare – \$282
 - for retail breach – \$131

Cost of lost business

- » Up 40 percent since 2005
- » 69 percent of overall cost (compared to 65 percent in a similar 2006 study)

Source: Ponemon Institute⁸

The dissolving perimeter and Web 2.0

As business has gone online and become vastly more mobile, the 20th century security strategy of protecting the organization's perimeter with firewalls, intrusion detection, and other similar tools has become insufficient. There are simply too many points of data entry and exit. While blocking the perimeter remains important, protection must focus on controlling access to the information.

This need is growing exponentially with the totally different perspective introduced by Web 2.0 users. This new “employee 2.0” workforce brings a mindset that is highly tuned to sharing information on social networking sites, posting to blogs, and emailing and IMing friends, with little or no regard to whether this is appropriate in a business context.

The challenge for today's DLP solutions

Several enterprise-focused DLP solution vendors, have developed innovative solutions for preventing the leakage of sensitive company information. Many of these products focus on identifying and categorizing all company data and then implementing corporate DLP policies to track sensitive information across the enterprise, applying controls where necessary.

These solutions make a lot of sense in concept, but in practice they run up against several implementation roadblocks.

- **Too much data, too little time.** For many organizations data is so dispersed, disorganized, and voluminous that classifying it comprehensively is just too burdensome and resource-intensive a task for most IT departments to undertake.
- **IT resistance.** Many available DLP products are relatively new and still suffer from issues such as frequent false positives. IT departments can be reluctant to invest their increasingly stretched resources in deploying another complex enterprise level infrastructure at the expense of delivering strategic value to the organization.
- **User resistance.** There is a wariness about deploying yet another agent on each desktop and laptop that might interfere with legitimate business by hogging processor cycles, requiring frequent updates and slowing down the performance of other user applications.

- **Complexity of scope.** Devising and implementing a comprehensive, viable policy to be supported by the DLP solutions can get in the way of regular business practices, requiring the involvement of not just IT but also human resources, finance and legal teams, and business unit managers.
- **The wrong focus.** Many of these solutions focus to a large extent on intentional data leakage, when in reality data leakage is hard to stop. For example, people can deliberately alter files to avoid detection or there is the more mundane problem of people simply sharing information inappropriately in conversation.

Organizations' real requirements

The truth is that, with the exception of the largest enterprises with the most stringent security requirements, most organizations simply don't have the funds, staff resources, and need to implement large-scale DLP efforts. Their most pressing and immediate needs fall into three categories.

Stopping the stupid

98 percent of data leakage incidents are actually due to accident or stupidity⁹ – as evidenced by three of the four examples on page 1. Lost laptops and USB keys, inadvertent misuse of email, the unthinking sharing of information on IM, webmail, social networking sites, and peer-to-peer file sharing sites are a much more significant threat to organizations than hackers.

Meeting regulatory requirements

The most pressing need for most organizations is to implement an effective solution that will satisfy auditors that they are providing the protection and control required to meet current regulations without the need for a huge amount of funds, staff, and resources in implementation and management.

Maximizing IT investment

IT departments want to ensure that the budget available to them – which is being asked to do more and more – is spent in the most efficient and cost-effective way. Solutions that integrate DLP with other security features are best placed to do this (as discussed more fully below).

Enabling DLP

Enforcing an acceptable use policy

Creating and enforcing an acceptable use policy (AUP) should underpin any attempts to stop data leaking from an organization. Because of the changing nature of both the organizational infrastructure and the expectation of employees that information should be freely available to access and share, an AUP's success depends heavily on creating ongoing employee buy-in to the fact that the threat is internal, overwhelming accidental, and in their hands to avoid.

Three steps to AUP success

- 1 Create the policy
- 2 Educate users about the policy
- 3 Enforce the policy

As well as stressing the importance of commonsense, the AUP should set out exactly how an employee is expected to use an organization's information, containing prescriptive advice on best practice and clearly defining prohibited behavior. It should cover issues such as:

- What information/files must not be emailed
- The company policy on posting to web message boards or downloading from the web



Organizations need to implement products that combine DLP features with other security functions to provide an integrated solution.



- The policy on use of USB keys and CDs for storing sensitive company information
- The policy on altering security settings.

The repercussions of not adhering to the policy should also be spelled out.

Integrated solutions

The key to achieving successful data leakage prevention within constrained budgets is to see it as part of your overall security picture, not as a separate entity. In fact, you might already have security tools with features that address your most pressing DLP requirements.

As DLP grows as a corporate concern these features are likely to be upgraded in much the same way that spyware prevention, spam detection, and intrusion prevention all started as separate security categories and infrastructures, but were quickly subsumed into other categories, such as anti-virus protection and firewalls.

As you go forward, the inclusion of up-to-date DLP features is something you need to ensure in order to make the most of your budget. The two key requirements can be summed up as:

- 1 Protect your data** against accidental loss or deliberate theft
- 2 Secure your data** so that if it *is* lost or stolen, it cannot be read.

Protect your data

Endpoint protection

Endpoint protection goes far beyond the imperative not to leave laptops on trains:

- Use powerful anti-malware solutions to block spyware that can steal financial and other confidential data.

- Block the use of non-essential applications such as P2P file sharing, IM, FTP clients, unauthorized email clients, wireless network connections, and smartphone and PDA synchronization tools. All of them can be subverted by criminals to get hold of information. Even more easily, employees can – usually unthinkingly – send out and share company data via these applications.
- Manage write access to portable storage devices such as USB keys. Because these are so easy to lose, these devices are a high security risk.
- Ensure that every computer connecting to the network – whether office-based or remote, company-owned or belonging to guest users – is compliant with the organization’s security policy.
- Controlling access to particular websites and applications and to webmail sites such as Gmail and Yahoo! Mail.
- Controlling and blocking the unauthorized use of IM and FTP traffic.
- Protecting against “drive-by downloads” which secretly place spyware on the user’s computer when they visit a website.

Gateway protection

Much of the functionality available in email and web products can prevent sensitive or inappropriate data being sent outside the organization or to unauthorized users inside the organization. Features include:

- Content scanning of email messages and attachments to control and block sensitive information, by identifying, for example, social security numbers, or keywords relating to confidential corporate information.
- Content scanning of web traffic to ensure spyware Trojans and other malware are not downloaded onto the user’s computer.
- Preventing the download of particular file types and preventing users from disguising and obfuscating unauthorized file types in emails.



If you’re not implementing encryption you’re just not doing your job.

Larry Ponemon, founder and chairman, Ponemon Institute¹⁰.



Secure your data

In spite of having the best policies and the best solutions, you might still find your data has been stolen or lost. So it is essential to have a second layer of defense – encryption. In a survey by the Identity Theft Resource Center, 82 percent of respondents who had lost data, said that if the data had been encrypted, the risk to the company would have been far reduced.² With this being the case, you should:

- Perform full disk encryption of laptops and notebooks.
- Encrypt data on removable storage devices, such as USB drives, CDs and DVDs.
- Encrypt emails to prevent unauthorized users from reading them.

Encrypting your data and devices in this way means that your information is safe, even if it gets into the wrong hands.

Summary

Data leakage has become one of the most pressing security issues facing organizations today. The most effective solution to the problem is to see DLP as part of your overall security problem, integrating it into a comprehensive strategy. You also need to create an AUP, enforce it with technology and ensure that both are monitored for compliance with corporate policies.

Sources

1. IDC, "Information Protection and Control Survey: Data Loss Prevention and Encryption Trends," Doc # 211109, March 2008
2. www.networkworld.com/news/2009/011409-encryption-told-to-stop-ignoring.html?fsrc=rss-security
3. edition.cnn.com/2008/WORLD/europe/06/11/alqaeda.documents.ap/index.html?iref=newssearch
4. www.sophos.com/blogs/gc/g/2008/11/05/bank-of-ireland-loses-customer-data-on-memory-stick
5. www.columbusdispatch.com/live/content/local_news/stories/2008/05/06/wooster.html?sid=101
6. www.sophos.com/blogs/gc/g/2008/09/23/second-tjx
7. www.myfoxdc.com/myfox/pages/News/Politics/Detail;jsessionid=68668DBA3F33BEAA644FC7D9A0D4CB6B?contentId=8055902&version=6&locale=EN-US&layoutCode=TSTY&pageId=3.14.1&sflg=1
8. www.encryptionreports.com/costofdatabreach.html
9. www.networkworld.com/news/2007/091107-data-leak-prevention.html
10. searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1294452,00.html

Sophos solution

Sophos Enterprise Security and Control provides complete protection for an organization's desktops, laptops, mobile devices, file servers, email gateway and groupware infrastructure, and all web browsing needs. It prevents data leakage by blocking malicious software and unauthorized applications and ensuring endpoint compliance. It also provides software or appliance protection at the email and web gateway. A full suite of encryption products from Utimaco, part of the Sophos group, offers a further layer of protection.

Boston, USA | Oxford, UK

© Copyright 2009. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM