Compliments of SOPHOS

Data Leakage FOR DUMMIES®

Sophos Special Edition

Protect your data, and monitor Web and e-mail use

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Lawrence C. Miller, CISSP

Data Leakage FOR DUMMIES®

SOPHOS SPECIAL EDITION

by Lawrence C. Miller, CISSP

WILEY

Wiley Publishing, Inc.

Data Leakage For Dummies®, Sophos Special Edition

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774

Published by Wiley Publishing, Inc., Indianapolis, Indiana

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For details on how to create a custom *For Dummies* book for your business or organization, contact `bizdev@wiley.com`. For information about licensing the *For Dummies* brand for products or services, contact `BrandedRights&Licenses@Wiley.com`.

ISBN: 978-0-470-44326-2

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

WILEY

Table of Contents

Introduction

Data leaks are a serious problem for organizations everywhere and stealing very sensitive information is, all too often, as easy as copying data to a USB thumb drive and walking out the door.

Intentional theft is just one aspect of the problem, however. Far more often, innocent and well-meaning employees lose very sensitive data stored on a laptop hard drive, a mobile phone or device, or a CD-ROM, which can be a very embarrassing and costly mistake for your organization. News stories of companies and organizations that have compromised customers' credit card data, private health records, or classified government information, are far too common.

Whether it's a lost laptop (left in a taxi cab) or human error (posting sensitive data on a public Web site), the consequences of data leaks can be devastating for everyone involved. Naturally, you don't want your organization to be the next big story — which is why you're reading this book!

About This Book

This book describes the business, legal, and technical aspects of data leaks. We look at the problem of data leakage, the business challenges it presents, the legal requirements for protecting private data, and the various technical solutions available from security companies such as Sophos.

Foolish Assumptions

We assume that you're reading this book because you need to understand and address a very serious problem for organizations worldwide (and perhaps more specifically, your organization) — data leakage — and you just can't wait for the movie to come out! Although this book will certainly make you aware of how your own personal data may be at risk, its focus is on corporate data security and specific technical solutions for the enterprise.

How This Book Is Organized

Each chapter in this book covers a different aspect of data leakage prevention. We begin with the what, where, when, and why, then finish with the ever so important — how.

Chapter 1: What Is DLP? provides some general background information, defines the problem, and addresses policies — not just revisiting them, but perhaps creating them. We also cover the importance of user awareness and training, and give you some good advice on practical process improvements you can make in your organization.

Chapter 2: DLP and Regulatory Compliance covers one of the main business drivers for corporate data leakage prevention programs — regulatory compliance. We help you navigate the legal landscape and identify which regulations matter most to your organization.

Chapter 3: Strategies for Data Risk Management is where you put your money where your, uh, data is! We help you classify your data, assess its value (to you and others), and determine an appropriate data-protection strategy based on that classification.

Chapter 4: Endpoint Security begins with the end in mind. No, this isn't some fatalistic approach to the subject — it's the realization that perhaps the most prolific risk to your company's private data is in the endpoints your users use — their laptops and PCs. We look at ways to protect the confidentiality and integrity of your data before your endpoint goes missing, using encryption, antivirus software, and application control.

Chapter 5: Device Management extends data leakage prevention beyond endpoints, to the devices that your users use to (inadvertently) extend your data vulnerability — mobile phones and devices, PDAs, external hard disks, portable USB storage devices, CD/DVD drives (optical media), and wireless devices (Bluetooth, infrared, and WiFi).

Chapter 6: Network and Gateway Security addresses data leakage risks in your corporate network, including via corporate and Web-based e-mail, and instant messaging.

Chapter 7: Ten (Okay, Six) Ways to Reduce Your Data Leak Risks offers some technical solutions to the issues presented in this book. You find out about encryption, device control, data monitoring, application control, anti-virus protection, and network access control.

Icons Used in This Book

Throughout this book, we occasionally use icons to call attention to important information that is particularly worth noting. Here's what to look for and what to expect.

REMEMBER

This icon points out information or a concept that may well be worth committing to your non-volatile memory, your gray matter, or your noggin' — along with anniversaries and birthdays!

TECHNICAL STUFF

If you're an insufferable insomniac or vying to be the life of a World of Warcraft party, take note. This icon explains the jargon beneath the jargon and is the stuff legends — well, at least nerds — are made of.

TIP

Thank you for reading, hope you enjoy the book, please take care of your writers. Seriously, this icon points out helpful suggestions and useful nuggets of information that may just save you some time and headaches.

WARNING!

"Danger, Will Robinson!" This icon points out potential pitfalls and easily confused or difficult-to-understand terms and concepts.

Where to Go from Here

Well, if you had pointy ears instead of a pointy chin (like the Dummies Man logo), you might say "logic clearly dictates that you turn the page and start at the beginning." Instead, we suggest that the needs of *you* outweigh the needs of the *many,* and this book has been written to meet your needs!

We recommend starting with Chapter 1, in order to set the foundation for the rest of the book and establish some key concepts and common terminology. From there, you might skip ahead to Chapters 4, 5, or 6, if you have a specific issue or area of interest you need to quickly address, or continue on to Chapters 2 and 3 to help you build the business case for a data leakage prevention program in your organization.

No matter how you choose to assimilate the information in this book, be sure to finish with Chapter 7, to learn how Sophos can help you "boldly go where no one has gone before" and avoid "the wrath of cons" — well, at least to address the very real challenges of data leakage prevention!

Chapter 1

What Is DLP?

In This Chapter

- Understanding data leakage and why it matters
- Exploring data, data, everywhere — at rest, in motion, and in use
- Defining the threat to your data and your organization
- Recognizing the importance of policies and user awareness training

As attitudes towards work and information continue to evolve away from those of the past, organizations have become more aware of the acute need to control the information that flows into, through, and out of their networks.

This need is growing exponentially with the totally different perspective introduced by the modern workforce. Technologically savvy employees use e-mail, Web browsing, social networking, and Web-based applications to improve their personal productivity whether working in the office, on the road, or at home. This mindset blurs the line between work and home with the effect that sending work home using a Web-based e-mail account, connecting to a home PC from work, sharing information on social networking sites, posting to blogs, and e-mailing and instant messaging (IM) friends, occurs frequently with little or no regard to whether it is appropriate or secure in a business context.

In this chapter, we talk about data leakage: what it is, where it occurs, why it matters, and some basic steps to prevent it.

Defining Data Leakage

After years of battling intrusions, viruses, and spam, organizations now find themselves wrestling with another growing security issue: *data leakage* — the intentional or accidental exposure of information ranging from legally protected personal information to intellectual property and trade secrets. Today's data security breaches encompass the wider IT environment, such as (in order of likelihood):

- Lost or stolen laptops
- Corporate and Web-based e-mail
- Flash disks, external hard drives, and USB thumb drives
- Optical media (CD/DVD)
- Other Web sites
- Social networking tools and other applications (such as IM and FTP)

The inadvertent exposure of confidential information has become the number one threat for many organizations today, particularly when financial data or personally identifiable information (PII), which may be protected by various laws and regulations, is exposed. *Information protection and control* (IPC) — defined as monitoring, encrypting, filtering, and blocking sensitive information contained in data in use, data at rest, and data in motion — is an important part of any overall data protection strategy. We describe data in use, at rest, and in motion later in this chapter.

The Growing Importance of DLP

Data leakage prevention has moved to the forefront of enterprise security for several reasons including bad publicity associated with data leaks, increasing government and industry regulations, rising incident costs, and greater exposure resulting from a more mobile workforce and porous network.

High-profile, reputation-damaging data leaks

Bad publicity from data leakage can result in damaged reputation, lost customers, and sometimes even ruin for companies that fall victim to such leaks.

The number of well-publicized examples of data security breaches is growing significantly. Recent high-profile incidents have included

- Between December 2007 and March 2008, hackers stole 4.2 million credit and debit card numbers from Hannaford Bros., a U.S. supermarket chain that has 165 grocery stores in the New England area.
- In September 2008, the city of Indianapolis, Indiana inadvertently posted the names, birthdates, and social security numbers of approximately 3,300 individuals on the city's new public Web site.
- In November 2007, Her Majesty's Revenue and Customs (HMRC) in the U.K. lost personal data — including birthdates, National Insurance numbers, and bank details — on 25 million people when two CDs sent by mail from the HMRC to the National Audit Office disappeared.
- In October 2008, a laptop computer containing the names, addresses, birthdates, and social security numbers of more than 5,000 individuals was stolen from the Fresno, California offices of KRM Risk Management Services.

Government regulations and PCI DSS

Governments everywhere and at every level have aggressively passed new regulations and legislation over the past several years to protect consumers from identity theft. These regulations often require specific controls, corporate compliance programs, audits, public disclosures, and stiff penalties for noncompliance. Examples include HIPAA and Sarbanes-Oxley (SOX) in the U.S. and the Data Protection Act in the U.K. Industries have also begun passing privacy rules and requirements such as the Payment Card Industry's Data Security Standard (PCI DSS). We take a closer look at government and industry regulations in Chapter 2.

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 and fines. All these costs have been rising steadily.

The disappearing network perimeter

As business has gone online and become vastly more mobile, the twentieth 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 securing the perimeter remains important, protection must focus on controlling access to the information, as well as controlling "guest" access (for example, contractors) to the network.

Now, we take a look at what data you need to protect.

Money out the door

Here are some statistics about the rising costs of data leakage incidents.

Cost of a data breach

- ✓ Up 43 percent since 2005
- ✓ Average cost per breach — $6.3 million
- ✓ Average cost per record — $197, for financial firms — $239

Cost of lost business

- ✓ Up 30 percent since 2005
- ✓ 65 percent of overall cost (compared to 54 percent in a similar 2006 study)

Source: *Ponemon Institute, November 2007*

Defining Data at Risk

Information protection and control (IPC) begins with defining what data is at risk within your organization. Broadly defined, this includes data in use, data at rest, and data in motion.

In use

Protecting *data in use* involves protecting the confidentiality and integrity of data while it is being accessed or modified.

Endpoint security helps to ensure that Trojans, keystroke loggers, and other malware don't compromise the confidentiality of your data. This includes anti-virus solutions to help protect the integrity of your data.

Equally important to ensuring the confidentiality of your data in use is end user security awareness and training. Social engineering is the easiest method for gaining access to confidential data. End users must be kept aware of current and evolving threats, as well as "common sense" steps — such as not working on confidential data in plain sight of others in a hotel lobby or airport terminal, for example.

At rest

Data at rest refers to data that is in storage. Most commonly, this refers to files and databases on computer hard drives including laptops, PCs, servers, storage area networks (SANs), and network-attached storage (NAS). Perhaps less apparent, data at rest also includes data on backup tapes or other offline or near-line storage media, archived data, data copied onto CDs, DVDs, and USB thumb drives; and printed data stored in more traditional file cabinets, vaults, desks, and briefcases.

In the context of data leakage prevention, data at rest is perhaps the biggest challenge for organizations. Organizations must first identify its data at rest. This task can be daunting because data is literally everywhere! Knowing where your data is stored, *everywhere* that it is stored, is an important first step — you have to know what you are protecting.

TIP

Knowing where your data is stored can also save you valuable time and money if your organization is subpoenaed in a litigation matter. Being able to quickly, accurately, and specifically quantify the costs associated with a discovery order may help your lawyers limit the scope of the order. Being able to confidently comply with the order, completely and accurately, will save your organization potential embarrassment, court fines, or a lost case because of "non-existent" data that is inconveniently discovered on a CD locked in a rusty safe in a corner of your datacenter.

Next, you need to know why you are protecting the data. This involves more than "because it's confidential" or "because it's the right thing to do." This is best accomplished with a data classification scheme that helps you place an implicit or explicit value on your data. This is necessary because it is simply not possible or effective to protect all data equally. We cover data classification techniques in Chapter 3.

In motion

Data in motion refers to data that is being transmitted across a network, such as a corporate LAN or intranet, a private extranet, or the public Internet. Data in motion is typically a more difficult target for hackers than data at rest because it is a moving target. Data in motion must be hijacked or intercepted and re-assembled, which requires much more skill than simply downloading the data from a compromised server or doing a little social engineering to get access through a blissfully unaware employee.

Data in motion is typically protected by securing the transport medium (the network) with virtual private networks (VPN) using IPsec or SSL/TLS encryption.

WARNING!

In this book, data in motion is defined as data that is being transmitted across a network. Other texts sometimes include data in motion as data on backup tapes or on CDs being physically transported to another location. However, limiting the definition to data being transmitted across networks provides a more focused context for our discussion of DLP strategies and solutions.

Next, we identify who may be a data leakage threat to your organization.

Identifying the Threat

Data leaks happen for many reasons, including good people doing not-so-good things, bad people doing bad things, and presumably "good" people (people we trust within our organizations) doing bad things — the good, the bad, and the downright ugly!

Good people doing not-so-good things

Unfortunately, good people often do things without thinking about — or being aware of — the consequences of their actions. Examples would be sending private customer data in an IM or e-mailing a confidential spreadsheet to your personal e-mail account so that you can work on it at home and impress the boss the next day. Although these actions may seem innocent enough, they are far too often the source of serious data leaks.

Bad people doing bad things

Cybercrime has become a lucrative cash cow for organized crime. No longer limited to hackers and script kiddies looking for bragging rights by defacing a popular Web page, cybercriminals target valuable data that can be used for fraud, corporate espionage, terrorism, or blackmail.

The "enemy" within

Perhaps nothing stings worse than when someone you trust betrays your organization. An inside employee with relatively unrestricted access to private data may be tempted to steal that data for personal gain in a new job, to sell to a competitor, or for vindictive reasons.

Finally, we discuss how to begin addressing the problem of data leaks by developing and implementing effective security policies.

The Importance of Policies in Data Leakage Prevention

Organizational policies should include various employment policies and practices, such as:

- **Pre-employment background checks:** Reference checks, verification of data in employment applications and resumes, and local law enforcement
- **Periodic post-employment screenings:** Credit checks and drug screenings may be appropriate for personnel with access to sensitive or financial information
- **Separation of duties and responsibilities:** To ensure that no single individual has complete control of a critical system or process, or full access to sensitive information

Creating and enforcing an acceptable use policy (AUP) should underpin any attempts to prevent organizational data leakage. A successful AUP depends heavily on creating ongoing employee buy-in to the fact that the threat is internal, overwhelmingly accidental, and in their hands to avoid. This is important because of the changing nature of both the organizational infrastructure and the employee expectations that information should be freely accessible and easily shared.

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 practices, and clearly defining prohibited behavior. It should cover issues such as:

- What can and cannot be done with company information/data
- What permissions are required to transfer company information, who is authorized to give that permission, to whom such information may be transferred, and by what means
- What information/files it is acceptable to e-mail
- The company policy on posting to Web message boards or downloading from the Web

- The policy on use of USB thumb drives 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.

Effective e-mail policies

While banning staff from sending or receiving personal e-mails is unrealistic, organizations can set boundaries that define reasonable, excessive, or inappropriate use through a comprehensive, updated, and enforced e-mail AUP. An e-mail AUP should not just address security and operational areas, but also compliance and data leakage definitions.

A framework for corporate governance

It is estimated that as many as 97 billion e-mails are sent worldwide every day! Governments around the world have responded to e-mail's growing use as a business-critical tool by introducing increasing levels of legislation governing the security, storage, and retrieval of e-mail. Falling afoul of such legislation not only damages an organization's reputation, but also can lead to fines, market de-listings, and — in extreme cases — prosecutions and prison sentences.

Keeping abreast of such legislation is challenging, and an AUP can help by providing a formal framework that is easily reviewed, audited, and enforced to ensure compliance. We take a closer look at laws and regulations in Chapter 2.

Preventing leakage of confidential information

According to IDC, e-mail is the number one source of leaked business information. Most of the time this can be accidental (thanks to e-mail client "features" like Auto-fill) with research showing that half of employees have sent a message containing sensitive or potentially embarrassing information by mistake. In addition, analysts at The Radicati Group have found that 77 percent of users have forwarded business e-mails to their personal accounts in order to complete work when away from the office. Even this most innocent of practices can leave an organization in breach of compliance regulations and can put sensitive information at risk.

Effective Web policies

Regulating Internet access in the workplace is a delicate balancing act. The Web provides employees with valuable information and tools that enhance productivity and competitive advantage, but it can also devastate business productivity with its endless supply of games, downloads, Web-mail, community and social networking sites, and online retailers. Other sources of risk include downloading pirated content, using social networking sites, and using Web-based e-mail or blogs to reveal sensitive information.

Building a workable policy

Technology awareness varies greatly in most organizations, as does understanding the business impact of Internet and e-mail abuse. Most employees know instinctively that watching YouTube videos wastes time, but many will not understand its true security, productivity, bandwidth, and legal implications.

The first step in creating an effective AUP is educating employees about the adverse effects of Web and e-mail abuse. Communication should include senior management, in addition to IT, and should encourage staff and business units to identify applications or Web sites that assist them in achieving the organization's goals.

The AUP should also match an organization's overall goals and philosophy. Organizations that give employees leeway in how they do their jobs will be better served by a policy that sets expectations and outcomes, emphasizing their spirit and the reasons behind them. On the other hand, organizations with a top-down management structure that defines tasks granularly will benefit from clear rules and regulations.

Regardless of the organizational philosophy, the policy should be written in a concise and easy-to-follow style. Language should be simple and the concepts relevant to each different department. It can also be useful to lay out a series of broad principles before concentrating on the finer details.

Chapter 2

DLP and Regulatory Compliance

In This Chapter

- Understanding privacy and data protection laws in the U.S. and Europe
- Talking about state disclosure laws
- Examining the Payment Card Industry Data Security Standards (PCI DSS)
- Getting acquainted with GLBA, SOX, and HIPAA

Governments worldwide have introduced increasingly stringent data protection legislation — such as the United States' Sarbanes-Oxley Act, Gramm-Leach Bliley Act, and HIPAA, and the United Kingdom's Data Protection Act — to provide suitable controls over sensitive information. Organizations found to be in breach of the legislation can be fined and forced to put solutions in place in order to prevent a recurrence.

Privacy and data protection laws are enacted to protect information collected and maintained on individuals from unauthorized disclosure or misuse.

Alongside government legislation, various industries, such as the Payment Card Industry (PCI), have implemented strict requirements for data security with contractually enforced penalties that can be every bit as stiff as government fines.

The U.S. Federal Privacy Act

The U.S. Federal Privacy Act of 1974 protects records and information maintained by U.S. government agencies about U.S. citizens and lawful permanent residents. Except under certain specific conditions, no agency may disclose any record about an individual "except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." The Privacy Act also has provisions for access and amendment of individual records by the individual, except in cases of "information compiled in reasonable anticipation of a civil action or proceeding." The Privacy Act provides individual penalties for violation including a misdemeanor charge and fines up to $5,000.

WARNING!

Although the Federal Privacy Act of 1974 pre-dates the Internet as we know it today, don't dismiss its relevance. The provisions of the Privacy Act are as important as ever and remain in full force today.

The U.K. Data Protection Act

The U.K. Data Protection Act (DPA) was passed by Parliament in 1998 and requires all organizations handling personal information about living persons to comply with eight privacy and disclosure principles, as follows. Personal data:

1. Shall be processed fairly and lawfully and shall not be processed unless certain other conditions (set forth in the Act) are met.
2. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and, where necessary, kept up-to-date.
5. Processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Shall be processed in accordance with the rights of data subjects under this Act.
7. Shall be protected against unauthorized or unlawful processing, and against accidental loss or destruction or damage, by appropriate technical and organizational measures.
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal information covered by the DPA includes names, birth and anniversary dates, addresses, telephone numbers, and e-mail addresses. For the most part, the DPA only applies to electronically stored information, although certain paper records used for commercial purposes may also be subject to the DPA.

DPA compliance is enforced by the Information Commissioner's Office (ICO), an independent official body. In addition to DPA enforcement, the ICO is also responsible for the Freedom of Information Act 2000. The ICO publishes DPA guidance for individuals and businesses available at `www.ico.gov.uk`.

For businesses that are subject to the DPA, you are legally required to:

- Notify the ICO that you are processing personal information (there is an annual £35 notification fee)
- Process personal information in accordance with the eight principles of the DPA
- Answer subject access requests received from individuals

WARNING!

Many U.K. businesses are targeted by fake "agencies" that claim to be official government offices. The scams often use threatening language, official-looking letterhead, and real U.K. mailing addresses. Typically, the scams will request sums of up to £135 to notify under the DPA. The ICO advises that you contact its hotline at 01625 545 740 if your business receives a suspected fraudulent letter.

Under the DPA, individuals have the right, among other things, to see any information about themselves held by an organization (called a "subject access request"), get incorrect information corrected, stop any unwanted marketing resulting from use of their personal information, and file a complaint against an organization they believe has breached the DPA.

TIP

If your business receives a subject access request, you should first determine whether any exemptions apply. You have 40 calendar days to respond to a request and can charge a fee of up to £10.

In addition to data protection laws, organizations must increasingly comply with disclosure laws that require you to "expose yourself" in the event of a data leak incident.

Disclosure Laws

The California Security Breach Information Act (SB-1386), passed 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.

The law is applicable to any organization that does business in the state of California — even a single customer or employee in California. Even if your company doesn't directly do business in California (for example, if your company stores personal information about California residents for another company), you are subject to the law.

Other states quickly followed suit and a total of 44 U.S. states now have similar public disclosure laws.

WARNING!

Although most state disclosure laws include statutory penalties, the damage to a company's reputation and potential loss of business — caused by the *public disclosure* requirement of these laws — can be most significant to companies that have protected data lost or stolen.

The Payment Card Industry Data Security Standard (PCI DSS)

Sometimes, the strongest motivation for compliance comes not from governments, but from industries themselves.

Although not a legal mandate, the Payment Card Industry (PCI) Data Security Standard (DSS) has far-reaching implications for businesses of any size, worldwide, that handle payment card (that is, credit card) transactions, including transmission, processing, or storage, to conduct business with customers. Compliance is mandated and enforced by the payment card brands (American Express, MasterCard, Visa, and so on) and each payment card brand manages its own compliance program.

Whether your company handles thousands of credit card transactions every day or only a single transaction a year, compliance with PCI DSS is required. Simply outsourcing your payment card processing transactions to a service provider does not satisfy your compliance requirement. Depending on the number of payment card transactions handled by your business each year, as well as other factors (such as previous data leak incidents), attaining compliance can range from conducting an annual self-assessment and network scan to onsite PCI data security assessments and regular (quarterly) network scans.

WARNING!

Failure to comply with PCI DSS can carry some heavy penalties levied by the payment card brands, including not being allowed to process credit card transactions (how would *that* impact your business?) and fines for non-compliance ($25,000 per month), as well as fines for violations that result in actual lost or stolen data (up to $500,000).

PCI DSS version 1.2 consists of six core principles, supported by 12 accompanying requirements, and more than 200 specific procedures for compliance. These include

- **Build and Maintain a Secure Network**

  Requirement 1: Install and maintain a firewall configuration to protect cardholder data

  Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- **Protect Cardholder Data**

  Requirement 3: Protect stored cardholder data

  Requirement 4: Encrypt transmission of cardholder data across open, public networks

- **Maintain a Vulnerability Management Program**

  Requirement 5: Use and regularly update anti-virus software

  Requirement 6: Develop and maintain secure systems and applications

- **Implement Strong Access Control Measures**

  Requirement 7: Restrict access to cardholder data by business need-to-know

  Requirement 8: Assign a unique ID to each person with computer access

  Requirement 9: Restrict physical access to cardholder data

- **Regularly Monitor and Test Networks**

  Requirement 10: Track and monitor all access to network resources and cardholder data

  Requirement 11: Regularly test security systems and processes

- **Maintain an Information Security Policy**

  Requirement 12: Maintain a policy that addresses information security

TIP

PCI DSS version 1.2 was published on in October 1, 2008 and though it doesn't introduce any new requirements, there are a number of clarifications around maintaining a vulnerability management program — in particular deploying anti-virus software on all operating systems that are commonly affected by malicious software. Version 1.2 became effective on the publish date with version 1.1 due to sunset on December 31, 2008. Go to `http://pcisecuritystandards.org` for the latest information on PCI DSS and a summary list of the changes to the standard in version 1.2.

Though enacted for different reasons, recent financial and healthcare regulations are also of significant concern for many organizations and often protect the same information as data protection laws. We discuss some of these regulations in the following sections.

The U.S. Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) opened up competition among banks, insurance companies, and securities companies. GLBA also requires financial institutions to better protect their customers' *personally identifiable information* (PII) with three rules:

- **Financial Privacy Rule:** Requires each financial institution to provide information to each customer regarding the protection of customers' private information.
- **Safeguards Rule:** Requires each financial institution to develop a formal written security plan that describes how the institution will protect its customers' PII.
- **Pretexting Protection:** Requires each financial institution to take precautions to prevent attempts by social engineers to acquire private information about institutions' customers.

Civil penalties for GLBA violations are up to $100,000 for each violation. Further, officers and directors of financial institutions are personally liable for civil penalties of not more than $10,000 for each violation.

The U.S. Sarbanes-Oxley (SOX) Act

In the wake of several major U.S. corporate and accounting scandals, the U.S. Sarbanes-Oxley Act of 2002 (SOX) was passed to restore public trust in publicly held corporations and public accounting firms by establishing new standards and strengthening existing standards for these entities including auditing, governance, and financial disclosures.

SOX established the Public Company Accounting Oversight Board (PCAOB), which is a private-sector, nonprofit corporation responsible for overseeing auditors in the implementation of SOX. PCAOB's "Auditing Standard No. 2" recognizes the role of information technology as it relates to a company's internal controls and financial reporting. The standard identifies the responsibility of Chief Information Officers (CIOs) for the security of information systems that process and store financial data and has many implications for information technology security and governance.

REMEMBER

SOX is only a requirement for publicly held, U.S. companies. However, voluntary compliance can be a useful feather in the cap for small, private B2B companies and non-U.S.–based international companies.

Although SOX does not mandate specific information security requirements, Sections 302 and 404 of the Act clearly establish the responsibility of a company's management and independent auditors to determine and certify that appropriate internal controls (including IT systems controls) have been established and are effective.

TIP

Because SOX does not establish specific IT security requirements, compliance can be tricky. Although no single set of standards can guarantee SOX compliance, the IT Governance Institute (`www.itgi.org`) and the Information Systems Audit and Control Association (`www.isaca.org`) provide excellent guidelines and resources to get you started.

The U.S. Health Insurance Portability and Accountability Act (HIPAA)

The U.S. Health Insurance Portability and Accountability Act (HIPAA) was signed into law effective August 1996. The HIPAA legislation provided Congress three years from this date to pass comprehensive health privacy legislation. If Congress failed to pass legislation by this deadline, the Department of Health and Human Services (HHS) was given the authority to develop the privacy and security regulations for HIPAA. In October 1999, HHS released proposed HIPAA privacy and security regulations entitled “Privacy Standards for Individually Identifiable Health Information.” Organizations that must comply with HIPAA regulations are referred to as *covered entities* and include

- **Payers (or health plan):** An individual or group health plan that provides, or pays the cost of, medical care; for example, insurers
- **Health care clearinghouses:** A public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements, such as data warehouses
- **Health providers:** A provider of medical or other health services, such as hospitals, HMOs, doctors, specialists, dentists, and counselors

WARNING!

Didn’t see your business in any of the preceding categories? Don’t worry, you haven’t been forgotten. Any person or organization that performs certain services for, or on behalf of, a covered entity that involves the use or disclosure of protected health information is defined as a *business associate*. Although HIPAA doesn’t directly require a business associate to comply, a covered entity must contractually ensure that any business associates it uses is, more or less, HIPAA compliant.

Civil penalties for HIPAA violations include fines of $100 per incident, up to $25,000 per provision, per calendar year. Criminal penalties include fines up to $250,000 and potential imprisonment of corporate officers for up to ten years. Additional state penalties may also apply.

Which Regulations Matter Most to Your Company?

The answer to that question is, quite simply: It depends. Unfortunately, there is no easy answer. That's why we have lawyers, and you absolutely shouldn't hesitate to contact your attorneys when dealing with matters of law. As you can tell from the broad overview given in this chapter, there are myriad factors to consider when determining which regulations matter most to your company or organization.

Some regulations only apply to government organizations, some apply to only specific industries, and some apply only in certain countries, states, or municipalities.

In general, you should begin by considering country or federal laws and regulations that typically supersede state and local laws. It is very likely that several laws and regulations will be applicable to your organization. You also have to consider those that may affect you only indirectly (for example, if you do business with a company that is subject to a given regulation). It is also very likely that there will be significant areas of overlap, conflict, and confusion. Work your way from the most specific guidance available to the least specific. In this way, you'll likely hit any areas of overlap and save valuable time and effort while covering all the bases.

In the next chapter, we turn our focus from the external environment (laws and regulations) to the internal environment (risk management, data classification, and security awareness and training).

Chapter 3

Strategies for Data Risk Management

In This Chapter

- Getting in touch with your sensitive . . . data: credit cards, financial data, trade secrets, e-mail contacts, and more
- Classifying your data so that your users know how to keep a secret
- Protecting information from beginning to end — the circle, uh, cycle, of life!

All data has some value to an organization — either intrinsic or extrinsic, or both. But all data is not created equal, and it's simply not feasible or effective to try to protect all data equally. Therefore, it is important to know what data is sensitive, private, or otherwise important to your organization, to classify it appropriately, and to safeguard it from the moment the data is created or received, throughout its existence, and until the end of its useful life — all of which we cover in this chapter.

A Little Sensitivity Training: Identifying Your Sensitive Data

Knowing what you're protecting and why you're doing so is important. Data is everywhere, and you might be (unpleasantly) surprised to find sensitive data in some unexpected places.

Credit cards, financial data, and customer information

Credit card information, sensitive financial data, and other *personally identifiable information* (PII) is commonly found on e-commerce Web servers, accounting and payroll systems, CRM applications, and in various organizational databases.

Other less apparent places that this data may be found include Web browsers and spreadsheets, perhaps even stored on a portable USB device. Data found in such places is perhaps most susceptible to data leaks. Although servers are often a hacker's preferred target, a lost laptop or a compromised Yahoo! personal e-mail account with a few Excel spreadsheets from the office can be equally damaging sources of data leakage for an organization.

Intellectual property and trade secrets

Intellectual property rights, including patents, trademarks, copyrights, and trade secrets, are protected by U.S. law, and agreed, defined, and enforced by various organizations and treaties worldwide. These organizations and treaties include the World Intellectual Property Organization (WIPO), World Customs Organization (WCO), World Trade Organization (WTO), United Nations Commission on International Trade Law (UNCITRAL), European Union (EU), and Trade-Related Aspects of Intellectual Property Rights (TRIPs).

An organization's intellectual property can often represent a significant portion of the company's capital (listed as intangible assets) and therefore, the company's overall value. Most significantly, these include *patents* and *trade secrets*.

A *patent*, as defined by the U.S. Patent and Trademark Office (PTO) is "the grant of a property right to the inventor." A patent grant confers upon the owner "the right to exclude others from making, using, offering for sale, selling, or importing the invention."

A patent is granted by the U.S. PTO for an invention that has been sufficiently documented by the applicant and that has been verified as original by the PTO. A patent is generally valid for 20 years from the date of application. The owner of a patent can grant a license to others for use of the invention or its design.

A *trade secret* is proprietary or business-related information that a company or individual uses and has exclusive rights to. To be considered a trade secret, the information must

- Be genuine, not obvious, and not generally known to the public.
- Have a competitive or economic advantage and, therefore, have value to the owner.
- Be reasonably protected from disclosure — this doesn't mean that it must be kept absolutely and exclusively secret, but you must exercise due care to protect it.

Unlike a patent, a trade secret and the specific details of that secret are not made publicly available, and thus a trade secret does not expire as long as it is kept a secret. Trade secrets are commonly protected by nondisclosure agreements (NDAs) and non-compete clauses in contracts.

TIP

A company can maintain a competitive advantage indefinitely with a trade secret as opposed to a patent, which only protects the invention for 20 years, assuming the company can keep the trade secret a secret.

Trade secrets are protected in the U.S. by the Economic Espionage Act (EEA) of 1996 at the federal level, and the Uniform Trade Secrets Act (UTSA) at the state level. Criminal penalties under the federal statutes include fines up to $10 million for organizations and imprisonment up to 15 years for individuals for the misappropriation *or acquisition of misappropriated* trade secrets. Civil penalties under UTSA include injunctions, actual, and punitive damages.

E-mail contacts

Although you may not necessarily think of e-mail addresses as sensitive or private data, an e-mail address book can be a treasure trove of data. Most e-mail clients do little or nothing to protect this information.

E-mail address books are favorite targets of virus writers. After infecting a laptop or PC, many viruses will download your address book and then replicate and e-mail itself to all your contacts using your e-mail address as the "known" sender. Your customers, friends, family members, and other contacts will not be pleased!

You may have received a mass mailing from one of your vendors in the past that was sent to all their customers. Or worse, you may have been one of those vendors that sent a mass mailing to your customers (when sending mass mailings you should *Bcc* your recipients instead of sending *To* your recipients). It doesn't take long to realize your mistake — inevitably, at least one of the hundreds of recipients you sent the e-mail to will click Reply to All and inform everyone else of your mistake — with only a hint of sarcasm. The resulting flood of e-mail threads usually irks more than a few of your customers, some of which may be inclined to instruct you to remove them from your mailing list — permanently. Equally important, you've just leaked your entire customer list to the world!

Privileged communications

Privileged communications can take on many forms including in person and telephone conversations, letters, faxes, and e-mail.

When discussing privileged information, whether in person or over the telephone, it is important to always be aware of your surroundings. As easy as it may be for someone to sneak a peek at your laptop monitor, it is even easier for someone to eavesdrop on your conversation. Or, if you are someone who has a "commanding presence," it may be impossible for others not to overhear — or tune out — your private conversations.

Real-time communications are also susceptible to electronic eavesdropping. With the increasing use of Voice-over-IP (VoIP), electronic eavesdropping has become easier and therefore may become more prolific — and without proper authorization, it is just as illegal.

Letters, faxes, and e-mails, which increasingly at least begin in electronic format, must also be protected against data leakage. Privileged communications in letters, faxes, and e-mails can be protected using encryption, public keys, and digital rights management (DRM).

File-level encryption (discussed in Chapter 4) protects the contents of documents, spreadsheets, and other confidential files.

Encryption can also be used to protect the transmission of privileged information, for example, by using secure file transfers, secure fax machines, and TLS (Transport Layer Security) for e-mail communications.

E-mails can be further protected using asymmetric (or public key) cryptography to protect the confidentiality and integrity of an e-mail and guarantee its authenticity.

A *secure message* is sent by using the intended recipient's public key to encrypt a message you are sending. Only the recipient has the private key that decrypts the message, thereby protecting the confidentiality and integrity of the message.

A *signed message* is sent by using your own private key to encrypt a message you are sending. The recipient then uses your public key to verify that the message was in fact sent by you. A signed message guarantees the authenticity of a message and its integrity (the message cannot be altered after it has been encrypted with your private key), but it doesn't protect the confidentiality (anyone can retrieve your public key to decrypt the message and view its contents).

A *secure and signed message* is sent by using the intended recipient's public key to encrypt a message you are sending, then using your own private key to encrypt the message. The recipient uses your public key to verify the authenticity of the message, then uses his own private key to decrypt the contents of the message.

Digital Rights Management (DRM) software allows a user to set permissions on e-mails or files. For example, you can restrict the ability of a recipient to forward or print an e-mail, or you can limit the number of times or the period of time that someone can view an e-mail or document.

Next, we take a look at how you can prioritize your data protection needs.

Classifying Your Classified Data

Information and data, in all their various forms, are valuable business assets. As with other, more tangible assets, the information's value determines the level of protection required by the organization. Applying a single protection standard uniformly across all an organization's assets is neither practical nor desirable.

A data classification scheme helps an organization assign a value to its information assets based on its sensitivity to loss or disclosure, as well as to determine the appropriate level of protection. Additionally, data classification schemes may be required for regulatory or other legal compliance.

Data classification techniques

Data classification techniques are typically implemented to protect information that has a monetary value, to comply with applicable laws and protect privacy, and to limit liability. Criteria by which data is classified include

- **Value:** This classification criterion is the most common in commercial organizations. It is based on monetary value or some other intrinsic value.
- **Age/useful life:** This is classified as information that loses value over time, becomes obsolete or irrelevant, or becomes common/public knowledge.
- **Regulatory requirements:** Private information, such as medical records subject to HIPAA regulations and educational records subject to the Privacy Act (see Chapter 2), may have legal requirements for protection. Classification of such information may be based not only on compliance but also on liability limits.

Descriptive labels are often applied to company information, such as *Confidential and Proprietary* or *For Internal Use Only*. However, the organizational requirements for protecting information labeled as such are often not formally defined or are unknown. Organizations should formally identify standard classification levels as well as specific requirements for labeling, handling, storage, and destruction/disposal.

Information lifecycle management

Organizations must manage information throughout the *information lifecycle* (information at its various stages or phases; also sometimes referred to as the data lifecycle):

- From the point it is created or received
- Throughout its use and storage
- Until it is archived or destroyed

TIP

Many different conventions are used to describe the information lifecycle, but no widely adopted standard exists. We'll keep it simple and intuitive here: Information has a beginning, a middle (or life), and an end.

Information lifecycle management is best achieved using a policy-based approach to implement effective processes and appropriate technologies in order to meet the organization's business goals and confidentiality/privacy requirements.

Information begins!

When information is initially created or received by an organization, policies need to be in place to provide clear direction about how the information should be protected.

A data classification scheme will help users to quickly and appropriately classify and safeguard information. Certain types of information (such as government or military information classified as *Top Secret*) may have restrictions on the type of computer it can be created or processed on (such as a Department of Defense Trusted System) and where it can be created or processed (such as in a secure facility).

Some types of information received from other organizations may be subject to a nondisclosure agreement (NDA) or other legal or regulatory requirements.

Information lives!

Once a life (of information) begins, it must be properly safeguarded until its end. Sensitive information must be protected at all times including, for example, when it is being stored, retrieved, viewed, modified, updated, transmitted, transferred, transported, discussed, printed, copied, backed up, and restored.

Here again, clearly established policies and an organizational data classification scheme will help reduce the risk of accidental or deliberate data leakage by helping end users identify appropriate operational and technical safeguards for information such as tracking, auditing, and reporting all changes.

Throughout its life, information should be regularly (or, in some cases, continually) evaluated to ensure that an appropriate classification has been assigned and proper safeguards are in place and effective. Information may become more sensitive or less sensitive over time, thereby warranting a change in classification. Information may also become obsolete or otherwise worthless to an organization, its competitors, and potential data thieves.

Information ends!

At the end of its useful life, information must be destroyed, disposed of, or archived.

Retention requirements for certain types of information should be clearly defined in policies to ensure regulatory compliance. Policies should also address proper destruction and disposal of sensitive or classified information, for example:

- ✓ Does the data need to be overwritten with 1's and 0's multiple times?
- ✓ Does printed data need to be cross-cut shredded and burned?
- ✓ What recordkeeping is required to document proper destruction and disposal?

Chapter 4

Endpoint Security

In This Chapter

- Ferreting out dangers to endpoint security
- Protecting your laptop
- Taking on the not-so-social "social engineer"
- Understanding anti-virus software
- Encrypting your data for maximum protection

We know some readers like to skip to the end of a good book, so we've hidden the end of this book right in the middle. Actually, in this chapter, we take a look at endpoints — specifically, laptops and desktop PCs — not the climatic ending of this book!

Threats Against Endpoints

In the not-too-distant past, endpoint security simply meant keeping your anti-virus software up-to-date. Much more focus was directed at protecting an organization's servers and network infrastructure. Not that the threats against servers and the network have become any less dangerous, but cybercriminals — and criminals in general — have shifted *their* focus to the endpoints. That's where end users do their work, and end users are not only your organization's greatest asset — they can also be its weakest link.

In fact, many consider endpoints to be the most vulnerable part of any organization's network. A recent global corporate Endpoint Assessment Test conducted by Sophos found that 81 percent of corporate endpoints failed basic checks such as missing anti-virus, firewalls, and security patches. Go to `www.sophos.com/products/free-tools/sophos-endpoint-assessment-test.html` for more information.

Endpoints include laptops and desktop PCs. Endpoints can also include mobile devices and phones, removable USB hard drives, and CDs/DVDs, but we limit our scope to laptops and desktops here, then cover these other devices in Chapter 5.

In addition to viruses, specific data leakage threats against laptops and desktop PCs (and end users) include spyware, Trojans, rootkits, and other malware, lost and stolen laptops, and social engineering.

A *rootkit* is malware that allows a hacker to take complete control of your system. Rootkits can lie hidden on computers and remain undetected by anti-virus software. Although new rootkits can be prevented from infecting the system, if you had any rootkits before you installed your anti-virus protection, they may never be revealed. Removing rootkits without compromising system integrity is particularly challenging and needs to be done with care.

You can download several free security tools from `www.sophos.com/products/free-tools` including the following:

- **Endpoint Assessment Test** to verify that service packs and patches are up-to-date; anti-virus is installed, current, and running; and a personal firewall is activated.
- **Threat Detection Test** to scan for malware that your anti-virus may have missed.
- **Anti-Rootkit** to find rootkits hidden on your system.
- **Application Discovery Tool** to scan your network for VoIP, IM, games, and other "useful" programs your end users may have downloaded and installed on "their" endpoints.

Laptop Security

We begin our discussion of endpoint security with laptops, because lost and stolen laptops have become the single most frequent computer security incident and are a major source of data leakage for organizations worldwide. It has been widely reported that approximately 12,000 laptops are lost in U.S. airports every week!

Although most laptop thieves are interested in the value of the hardware, rather than the data on the laptop, organizations must prepare for and expect the worst when a laptop is stolen. Most data protection laws (see Chapter 2 for more information) now require public disclosure when individual private data is potentially compromised — such as when a laptop is lost or stolen. However, if the data was properly encrypted, many laws recognize that the data is still protected and therefore do not require costly and embarrassing public disclosures in such cases. We discuss encryption later in this chapter.

Since physical theft of laptops is so common, it seems logical to begin with physical security.

Today, laptops are everywhere and hardly anyone notices when you turn on your laptop to work on a few e-mails in a busy airport terminal while waiting for your flight. Hardly anyone, that is, except the opportunistic thief waiting for that fleeting moment when you are briefly distracted. Then, your laptop and the thief inconspicuously disappear into a crowd of people, all carrying more or less identical black laptop cases.

With any luck, you've only lost a $1500 laptop. But if you haven't taken appropriate precautions, you can't be sure that your company's, your customers', or your own confidential or private data won't end up posted on the Internet. And, if you were carrying around the construction plans for the Death Star on your laptop — well then, you may have just single-handedly brought about the end of our civilization!

Some commonsense tips and not-so-obvious physical security measures for laptops include the following:

- ✓ Always keep your laptop close when using or carrying it in public.
- ✓ Be aware of your surroundings at all times; thieves and con artists are everywhere and are usually more skilled at perpetrating crimes than you are at recognizing and defending against them.
- ✓ If you must leave your laptop in your car, lock it in your trunk — and, while you're at it — lock up your portable GPS device, removable satellite radio, iPod, and any other expensive gadgets that might tempt a thief to break your window.

- Never put your laptop in checked baggage at the airport. And, be sure you pick up *your* laptop after it passes through the security X-ray.
- Never write your password down. If you do it anyway, at least be sure it's not taped to your laptop or folded away in your laptop bag. Although a thief may just be after the hardware, giving away your password is just too inviting and easy for even the most common thief.
- In addition to the manufacturer's serial number, permanently attach or engrave an organizational identifier to the laptop in a conspicuous place. The tag should clearly identify what organization the laptop belongs to and ideally might include return and reward information. This makes it much harder for the thief to sell it to a pawn shop and somewhat easier for the police to identify it as stolen equipment.
- Use a security cable and lock to secure your laptop in your office or car. Some security cables and locks incorporate motion-activated alarms that can sense excessive motion or cut cables.
- Install laptop security tracking software. This software sends a heartbeat back to the organization or a managed security service when a lost or stolen laptop connects to the Internet. The laptop data can then be remotely erased and its physical location possibly even tracked.

Social Engineering

Despite all the notoriety attributed to hackers, script kiddies, and other classes of cybercriminals, social engineering remains one of the simplest and most effective methods for gaining unauthorized access to a system and/or stealing data. *Social engineering* is simply a fancy term for your common thief or con artist's typical tricks: it can be as low-tech as shoulder surfing (looking over your shoulder) or dumpster diving (digging through your trash), or as sophisticated as an elaborate e-mail or phone scam designed to solicit private data (such as passwords, financial data, and personal information) from unsuspecting end users. Your best defense against social engineering attacks is user awareness and training. Your users should know that:

- Your help desk will never ask for your password — so if someone calls you claiming to be from your organization's help desk and asking for your password, hang up and report the call to your IT department.
- Common thieves and corporate spies are not above going through your trash — so always shred sensitive or private data.
- People are naturally curious — or downright nosy — so always be aware of who is around you and who is watching your monitor or keyboard.

Anti-Virus Protection

Long gone are the days when computer viruses did little more than frustrate users by rearranging their desktop icons or rolling an annoying ambulance across their monitor screen. Viruses today are more prolific, destructive, and sophisticated than ever before. Malware (including viruses) is designed to steal information and provide back-door access to systems.

Anti-virus software is as important as ever in providing comprehensive security for endpoints. Anti-virus protection includes signature-based and heuristics-based software.

Signature-based anti-virus software is the most common anti-virus software in use today. Anti-virus signature files are developed by security vendors to detect and prevent *known* virus threats and are typically downloaded to servers and individual systems automatically on a predetermined schedule, perhaps daily or as often as every 15 minutes. Signature-based anti-virus software is effective, but largely reactive, in its approach. Some limitations of signature-based anti-virus software include

- As the number of viruses, worms, and Trojans has grown rapidly over the years (now more than one million), so too has the size of signature files. This is increasingly resource intensive in terms of network bandwidth, computer storage space, and processor/memory utilization.
- Because signatures are developed for *known* threats, there is usually a lag when new threats, known as *zero-day* or *zero-hour* threats, emerge. This lag (several hours

> or days) exists because a new threat that is “released into the wild” must first be detected and studied. Then a solution must be developed, tested, distributed, installed, and executed.

Heuristics-based anti-virus software uses a more proactive approach than signature-based anti-virus software to detect and prevent computer viruses. Heuristics-based software monitors normal operating system and application behavior to determine whether unusual activity or anomalous behavior that may possibly be associated with a virus occurs, then prevents its execution. For example, launching Notepad in Windows should not normally open a stealth connection to the Internet and transfer files to a server located in Nigeria. This could be a strong indication of a virus or other malware, which a heuristics-based anti-virus solution would prevent from executing.

Heuristics-based software analyzes the behavior of code at two stages:

- **Pre-execution.** Behavior of code is analyzed before it runs and is prevented from running if it is considered to be suspicious or malicious.
- **Runtime.** Intercepts threats that cannot be detected before execution.

Many anti-virus solutions today incorporate both signature-based and heuristics-based strategies to protect against known and emerging virus threats. In addition to anti-virus protection, a comprehensive endpoint security solution should protect against spyware, adware, Trojans, and rootkits. These threats are often unwittingly installed on endpoints through unauthorized applications, which we discuss in the next section.

Application Control

Application control software blocks or restricts the use of unauthorized applications that may adversely impact network performance, user productivity, or system security, such as instant messaging (IM), peer-to-peer (P2P) file sharing, Internet games, VoIP clients, and other potentially unwanted applications (PUAs). Such applications may be used to intentionally or accidentally leak data.

PUAs are applications that, while not malicious, are generally considered unsuitable for business networks. The major PUA classifications are adware, dialer, non-malicious spyware, remote administration tool, and hacking tool. However, certain PUAs might be considered useful by some users.

An application control solution scans a system and detects installed applications, then compares the detected applications against a security policy to determine which applications are permitted or restricted for a given user or group of users.

You can download a free Application Discovery Tool from `www.sophos.com` to scan your network for consumer applications. The tool operates alongside your existing anti-virus software and can help you identify and locate unauthorized applications on your network.

Effective application control solutions must also address applications that can be executed from removable USB drives or flash disks without administrator permissions.

Protecting Endpoints with Enterprise Encryption

Encrypting your data will help ensure your data remains safe from disclosure and your organization remains safe from costly and embarrassing data leakage liabilities, in the event that a laptop or other endpoint ends up lost or stolen.

Encryption is the process of converting plaintext data into unreadable ciphertext using a known algorithm and a secret encryption key.

An encryption key is nothing more than a password or passphrase. End users need to choose strong encryption keys and protect them. Writing an encryption key on a sticky note and sticking it under your mouse pad or on your laptop is a bad idea!

Encryption has become the preferred method for protecting data. Many data protection laws and industry regulations (for example, PCI) have been updated to address the use of encryption as an acceptable safeguard against data loss or leakage. If you can prove that your lost data was appropriately encrypted, in many cases you can avoid statutory public disclosure requirements and limit the liability associated with a data leakage incident.

Although encryption has become common worldwide, not all encryption algorithms are created equal. Many countries have laws that strictly prohibit the export of specific encryption algorithms and technologies. You can be held criminally liable and face criminal penalties if you "accidentally" bring your encrypted laptop on a business trip to a restricted country. Check with your IT department *and* your legal department if you use encryption technology and travel internationally.

Full-disk encryption

Full-disk encryption (FDE), also known as whole-disk encryption, encrypts the entire contents of a hard drive using a software-based or hardware-based encryption system.

Hardware-based encryption systems are typically faster than software-based encryption systems because they don't require CPU processing power or memory. Thus, data residing in memory isn't vulnerable to data leakage on hardware-based systems. Instead, encryption is accomplished on the hard drive itself (HDD FDE) or on a separate chipset (still largely under development).

Software-based full-disk encryption systems do not encrypt the Master Boot Record (MBR) of a disk and are therefore vulnerable to MBR viruses and rootkits. However, gaining access to properly encrypted data, via an MBR vulnerability, is *extremely* difficult, making the risk *extremely low*. Still, if your data requires *absolute* protection, consider using a hardware-based encryption system that also encrypts the MBR.

FDE has many advantages for individual end users and organizations seeking to protect data, including

- **Ease of use.** The end user doesn't need to do anything — such as deciding which files to encrypt or not to encrypt — everything on the disk is automatically encrypted, including temporary files and swap-space memory.

- **Centralized management.** Enterprise FDE solutions provide many useful management functions such as key recovery and destruction, policy creation and enforcement, and auditing and compliance reporting.
- **Pre-boot authentication.** Data encrypted with a secret key that is protected by the operating system's security mechanisms (such as a Windows logon) is just as vulnerable as if it were not encrypted at all. Many enterprise FDE solutions incorporate pre-boot authentication to eliminate this vulnerability.

Although ease of use is generally a significant advantage, it can also lull users into sloppy and unsafe work habits. For example, users may forget, or may not realize, that files are decrypted when they are copied to a removable USB thumb drive or sent via e-mail.

For even better data protection, some FDE solutions also support the Trusted Platform Module (TPM) security specification. A TPM security device is a cryptoprocessor that is embedded on the motherboard of some hardware devices, such as laptops. An encryption key can be tied to the TPM device of a laptop, which in effect ties the hard drive to the laptop. If the hard drive is removed from the original laptop, it can *never* be decrypted. The laptop is useless to its "new owner" without the original hard drive that's associated with the TPM device.

The extra security provided by a TPM device can also be a single point of failure. For example, if the laptop hardware has a problem, the hard drive cannot be simply installed in another laptop.

File-level encryption

File-level encryption is used to encrypt individual files or folders. File-level encryption systems can automatically encrypt all files in a certain directory (for example, My Documents) or can be used to manually encrypt individual files. File-level encryption also allows end users to create different encryption keys for different files for additional security (and complexity).

WARNING!

Password protecting a file is not the same thing as encrypting a file — not even close! A password simply (and temporarily) restricts access to a file. A “password-protected” document or spreadsheet can be easily cracked using freely available tools on the Internet.

Unlike full-disk encryption, file-level encryption typically does not encrypt the directory structure or other information, such as the name of a file or when it was last modified. This information, known as *metadata,* can be very useful to a data thief.

TIP

File-level encryption can be used in conjunction with full-disk encryption to further enhance data protection. Full-disk encryption systems generally use the same key to encrypt all data on the disk. Thus, if an attacker gained access to the key, he could theoretically access all the data on the hard drive (at that point it would only be protected by the user level security provided in the OS). With file-level encryption, each user on the system can have different keys, or a single user can have multiple keys.

Endpoint Compliance

An endpoint compliance solution should check connected laptops and PCs to ensure that they’re compliant with corporate security policies, and fix, quarantine, or otherwise isolate noncompliant endpoints. Endpoint compliance helps to prevent configuration drift and reduce DLP risk, for example, due to employees turning off firewalls and anti-virus software. We cover endpoint compliance in greater detail in Chapter 6.

Chapter 5

Device Management

In This Chapter

- Recognizing the dangers of USB devices, external hard drives, and optical media
- Keeping your mobile phones, Blackberries, and wireless networks secure
- Encrypting devices to prevent data leakage

Although many people used to laugh at those of us who carried around phones, pagers, PDAs, Walkmans, and maybe a few floppy disks in our utility belts, mobile devices have practically become the newest fashion trend. Mobile phones and Blackberries are everywhere, and USB devices have largely replaced bottle openers on key chains (some USB devices even double as bottle openers!). And, while all these fashionable, "hip" (pardon the pun) devices may be incredibly convenient and greatly enhance your productivity, they also significantly increase the risk of data loss and theft.

In this chapter, we take a look at all these neat little gadgets, the data leakage headaches they may cause, and what you can do to reduce the associated risks.

Restricting Storage Devices and Removable Media

Organizational policies need to address the use of removable media and portable devices to ensure data is not lost or stolen, malware is not introduced into the organization's network and systems, and acceptable use policies are properly enforced. Controlling which devices can be connected to an organization's endpoints — and for what purposes — significantly reduces an organization's risk for data loss. For example, restricting the use of generic USB devices and instead requiring encrypted flash disks, helps ensure that data cannot be copied from an endpoint unless it is properly encrypted on the flash disk.

USB devices

USB devices (also known as flash drives, thumb drives, memory sticks, and so on) have become prolific in our modern world. These devices are wildly popular because they are durable, reusable, easy to use, convenient, and inexpensive.

And, for all of these reasons, USB devices also pose a significant data leakage threat for organizations. In addition to an acceptable use policy addressing what types of information can be stored on USB devices or whether USB devices are even permitted, organizational policies should require certain operational and technical safeguards — for example installing software that restricts the use of USB ports on PCs and laptops, encrypts certain files automatically when they're copied to USB devices, and logs all file activity to or from a USB port.

WARNING!

Although you may not think of an iPod as a typical USB device, it is nonetheless another potential data leakage risk. Data files and multimedia content can be stored on an iPod almost as easily as on any other USB device and therefore should also be addressed in your organizational policies.

External hard drives

External hard drives, with capacities now up to 1 terabyte or more, are also readily available to end users and present yet another potential data leakage risk for organizations.

External hard drives typically connect to a laptop or PC through a USB or FireWire interface. Although not as portable as USB devices, external hard drives can have extremely large storage capacities and built-in redundancy capabilities (such as RAID protection) that make them extremely popular among end users.

External hard drives perhaps present more of a risk of data loss than data theft, because they're not as stealthy as USB devices. End users may have good intentions when using external hard drives, such as backing up valuable information or not wanting to use expensive company storage resources to store their entire MP3 collection. Still, it doesn't take much effort to hide an external hard drive in a briefcase, backpack, or coat pocket, and walk out the door.

CD/DVD drives — optical media

Although CDs and DVDs are losing popularity to USB devices, they remain a ubiquitous data leakage threat for organizations. CDs and DVDs still pose a significant data leakage threat because:

- Although not as versatile as USB devices, CDs and DVDs still have large storage capacities, up to 870 megabytes and 8.54 gigabytes, respectively. More than enough to store a few million credit card numbers.
- USB devices are getting all the attention so a potentially overlooked CD or DVD may be the preferred medium for a data thief in a given situation.
- CDs and DVDs cannot be easily destroyed, erased, or formatted. Far too often, a CD or DVD is simply broken in half and tossed in the trash — but the data is still there and recoverable to a motivated data thief.
- Accidental data loss, for example, due to a CD or DVD being left in a CD/DVD drive, is far more likely than with USB devices, which tend to be a little more obvious dangling off a laptop's USB port!

Organizations should implement policies that restrict optical media drive on endpoints to read-only access in order to prevent data from being copied to blank CD-Rs and DVD-Rs.

Mobile and Wireless Devices

It wasn't that long ago that a phone was just a phone. At best, it stored your contacts and your grocery list, synced with your calendar, and included a calculator and a few games.

Today, mobile phones, smart phones, mobile devices (such as Blackberries), and PDAs have become core business productivity tools, with as much functionality as many people require in a laptop or PC. The freedom of not being "wired in" makes these devices incredibly useful and popular.

Extending the convenience of wireless connectivity to laptops, PCs, and mobile or portable device of every sort, using Bluetooth, Infrared (IrDA), WAP (Wireless Application Protocol), and WiFi, further increases the functionality and popularity of these devices, as well as the data leakage risks and opportunities for data theft.

Mobile phones and PDAs

Smart phones, mobile devices, and PDAs have become standard business tools, storing sensitive business information and enabling e-mail on the move. This makes them an inviting target for malware and attackers seeking new ways to defraud users and steal confidential business data. Threats include data theft, disruption of mobile phone networks, phone hijacking, and malicious mobile code (such as worms that spread themselves via the mobile network).

To protect data on mobile devices, organizations should ensure that their security policy includes a strategy for mobile devices, covering:

- **Threat management.** Identification and removal of viruses, spyware and spam
- **Device access control and management.** Enforcing a password policy and application management
- **Data protection.** Encryption of sensitive data on devices and remote data deletion
- **Network access control.** Controlling VPN connections across public networks and validation of devices when they connect to the corporate network

Bluetooth

Bluetooth is a wireless protocol, commonly used on mobile devices to create a personal area network (PAN). Bluetooth technology has become prolific in the ten years since being developed, and it now ships on more than two billion products worldwide.

As with many wireless protocols, Bluetooth for the most part is inherently insecure. Security risks include Bluejacking and Bluesnarfing attacks. *Bluejacking* is sending anonymous, unwanted messages to other users with Bluetooth-enabled mobile phones. *Bluesnarfing* is the theft of data from a Bluetooth phone.

To reduce the risk of attacks, users should turn off Bluetooth or set it to "undiscoverable". The undiscoverable setting allows you to continue using Bluetooth products like headsets, but means that your phone is not visible to others.

IrDA

Although decreasing in popularity (largely due to Bluetooth), many mobile devices are still equipped with infrared ports (IrDA, or Infrared Data Association). IrDA is a short-range line-of-sight protocol used to transfer data using infrared light. Ranges are typically limited to 1-meter or less, and the communicating devices must remain more or less stationary.

Although IrDA use is declining, it still presents a data leakage risk to an organization's mobile users, particularly given its high data transfer rates (up to 16 megabits per second) and relatively low attention given to IR port security by organizational IT staff, security vendors, and professionals.

Wireless Application Protocol (WAP)

WAP is primarily used to enable Internet access on mobile phones and devices. Web sites that support WAP browsers use the Wireless Markup Language (WML) to format Web pages for the smaller screens of mobile devices. The *Wireless Transport Layer Security* (WTLS) protocol provides security services for WAP.

Do not confuse the Wireless Application Protocol (WAP) with Wireless Access Points (also abbreviated WAP). The Wireless Application Protocol is used to enable Internet access on mobile devices. Wireless Access Points are used on WiFi networks to connect wireless devices to a wired network.

WiFi

Much of the attention on WiFi security has been focused on vulnerabilities associated with WEP (Wired Equivalent Privacy) and SSIDs (Service Set Identifiers). Far too many organizations still use WEP and default SSIDs (or descriptive SSIDs, for example “store#0803”). Retail stores and hotels have become a favorite target for attackers attempting to steal credit card information from wireless POS (point-of-sale) systems and networks.

To protect your organization’s wireless networks, you should use WiFi Protected Access (WPA or WPA2) to provide authentication, confidentiality, and integrity. If pre-shared keys are used with WPA, the keys should be protected and strong — and changed frequently. If possible, use MAC address filtering to restrict the devices that can connect to your wireless network and do not broadcast SSIDs.

Device Encryption

Similar to full-disk encryption and file encryption products (described in Chapter 4), device encryption software protects the contents of mobile devices, USB removable hard drives, and flash thumb drives by transparently encrypting data stored on these devices. Encryption can occur at the sector-level or file-level, or a combination of both.

Chapter 6

Network and Gateway Security

In This Chapter

- Protecting corporate and Web-based e-mail
- Understanding the dangers of instant messaging
- Working with Network Access Control — at the gateway, in the data path, and on the network
- Securing endpoints with Endpoint Compliance

Protecting IT networks used to be a straightforward case of encircling computers and servers with a firewall and ensuring that all traffic passed through just one gateway. However, the increase in mobile workers, the amount and types of devices, and the number of non-employees (such as contractors, vendors, and temporary workers) requiring network access has led to a dissolving of that network perimeter. Access requests can come from anyone and anywhere, and organizations must now address data leakage threats throughout the network.

Corporate and Web-Based E-mail

It is impossible to imagine business without e-mail. However, the proliferation and ease of use of e-mail opens it to abuse. Spammers bombard users with unsolicited messages and organized cybercriminals systematically use e-mail and zombie networks (botnets) to disseminate malware and commit identity theft.

Organizations also need to ensure that their own employees use e-mail systems appropriately. The spread of dubious content and malware via e-mail has the potential to cause offense and reflects negatively on an organization. Inadequate protection of the e-mail infrastructure no longer just costs businesses in terms of time, but also leads to bad public relations, lost revenue, damaged share prices, and financial penalties in the form of fines and lawsuits.

Further, it is estimated that as much as 80 percent of an organization's operational records are stored within the e-mail infrastructure, and so it's easy to see how business-critical data can fall into unauthorized hands.

As the continued growth in external threats is compounded by internal threats, an e-mail security solution must serve a dual purpose:

- Block spam, phishing, and malware attacks
- Ensure that organizations control their sensitive information (such as private customer data and intellectual property) and avoid costly compliance mishaps.

Overview of the e-mail infrastructure

E-mail is a system constructed of multiple components that play differing roles. To ensure that each component delivers maximum performance, e-mail security must also take a multilayered approach. A basic e-mail infrastructure consists of the following components:

- **E-mail gateway.** Also known as the e-mail boundary or perimeter. This is the first line of e-mail contact between your organization and the outside world. It is the point through which all inbound and outbound e-mail travels.
- **E-mail server.** In addition to all inbound and outbound e-mail, the e-mail server handles all internal e-mail and acts as a storage depot for mail not yet downloaded by the e-mail client.
- **Endpoint.** The desktops and laptops and other devices (such as Blackberries and mobile phones) that run e-mail clients.

The inbound threat

In terms of volume, the most significant threat to the e-mail infrastructure comes from external spammers and cybercriminals. These individuals have long used e-mail to advertise their merchandise and breach security defenses, and are constantly adapting their tactics in an attempt to bypass current security measures.

Spam

Spammers use increasingly creative ways to obfuscate their sales pitches, hiding them inside attachments, images, or even audio files. Such techniques attempt to bypass traditional e-mail filters, providing spammers with an unobstructed path to user mailboxes.

Spammers have also become very adept at using social engineering to disguise the true content of a message in order to trick recipients into opening it and clicking on a Web site link contained in the e-mail. Users may think they're accessing a YouTube video, e-card, or software upgrade, but they may end up accessing a Web site selling generic pharmaceuticals or counterfeit branded goods. "Pump-and-dump" campaigns are also increasing in popularity. This scam technique talks up a public company's prospects in order to falsely inflate its share value, allowing spammers to sell their shares and realize a substantial capital gain.

Phishing, spear phishing, and whaling

Phishing involves sending out e-mails that appear to come from reputable retailers, banks, or credit card companies. These e-mails lure victims to fake Web sites that are almost exact replicas of the real site. From there, criminals capture usernames and passwords, bank account numbers, and PINs.

Spear phishing is a phish attack launched at a specific organization. An e-mail appearing to come from a trusted source (such as the CEO, the human resources manager, or an IT systems administrator) tricks employees into providing network passwords, intellectual property, and confidential data.

Whaling is a highly targeted phish attack directed at a high profile individual, such as a journalist, celebrity, or business leader.

Malware and blended threats

The days of the e-mail virus readily identifiable by its suspicious .exe or .zip attachment are in decline (but not gone or forgotten). Cybercriminals have instead adopted more sophisticated techniques for infiltrating corporate networks. A popular tactic is to spam out e-mails containing Web site links that point recipients toward Web sites hosting malicious code. These e-mails contain no malware themselves, and so are more likely to bypass perimeter defenses.

Directory harvesting

Hackers use directory harvesting to probe an organization's e-mail server, guessing at e-mail names and formats in order to gather bona fide addresses, which they can either use or sell to other cybercriminals. The sheer number of server requests — and subsequent non-delivery reports — can, in extreme cases, cause an e-mail server to fail, leaving the organization without e-mail.

Inappropriate content and PUAs

Most organizations accept the occasional use of their e-mail systems for personal reasons. However, there is a risk that personal e-mails can harm the organization's reputation or expose the organization to legal liability if an employee is sending or receiving pornographic or threatening content, or operating a "small, home-based" business using your corporate e-mail system and e-mail domain. Incoming personal e-mails can also add extra strain to the network, especially if they contain large music, gaming, or video files. *Potentially unwanted applications* (PUAs) such as remote access tools and automatic dialers, can also be difficult to manage and drain network resources.

The outbound threat

E-mail leaving networks is smaller in absolute volume than incoming messages, but it poses similar risks in terms of security and compliance, and a greater risk in terms of data leakage.

Inappropriate content

Few organizations will allow pornography or other offensive content to be sent from their network, but the threat can come from more innocent sources. Family photos and videos, links to non-business Web sites, and other personal content consume bandwidth and can negatively affect the image of the company if sent to unintended recipients.

Data leakage

E-mail is one of the major sources of leaked business information and these leaks are usually accidental. For example, many e-mail clients use an auto-complete feature when typing names in the To: field, for convenience. However, this feature makes it easy to inadvertently add an unintended recipient. It is not uncommon to send an e-mail containing embarrassing or sensitive information to the wrong recipient by mistake.

Additionally, it has been estimated that as many as three of every four business users have, at times, forwarded business-related e-mail to their personal or Web-based e-mail accounts. This might help employees work more flexibly but, more ominously, it also facilitates data theft (such as corporate espionage or preparing to change jobs) and represents a significant hole in the organization's defenses. It is particularly challenging for firms operating in highly regulated industries.

Botnets

Hijacked computers can become part of a botnet and, unknown to their owner, launch malware, spam, or distributed denial of service (DDoS) attacks. Botnets impact network processing speeds and damage reputations, as offending messages will appear to come from a legitimate source. In extreme cases, an organization can find its domains and/or IP address ranges are blocked by service providers and other organizations.

The internal threat

Many outbound and inbound threats are also found in internal e-mail. Data leakage between departments, circulation of inappropriate content, and distribution of non-essential applications all put e-mail infrastructures at unnecessary risk.

Additionally, the rise of regulatory compliance governing the security, storage, and retrieval of information also has a direct impact on e-mail use. With e-mail often acting as the "corporate memory," businesses must adopt strategies that keep information safe and easy to locate. Under many countries' laws, organizations are obliged to keep all recorded communications, including e-mail. If they are later required in court, the absence of archived e-mails will be regarded as negligent.

A four-step approach to e-mail defense

A logical four-step approach to defending your organization's e-mail infrastructure consists of protecting the gateway, defending the e-mail server, securing the endpoint, and controlling access to the network.

Protect the gateway

The central pillar in the defense against e-mail security threats is gateway protection, which should scan all inbound and outbound messages.

The anti-spam engine must be able to detect and block (or quarantine) new and emerging threats (including spam, phishing attacks, viruses, spyware, and other malware) using techniques such as reputation filtering, pattern matching, URL detection, and image and attachment fingerprinting. The best solutions will provide proactive protection against new (zero-day) threats, even before specific detection rules can be developed.

What is a botnet?

What exactly is a botnet? Read on.

- A botnet is a centrally controlled network of "zombie" computers that hackers have infiltrated to perpetuate malicious acts.
- Hackers use the combined processing power and distributed Internet bandwidth of multiple zombies to send out spam or phishing campaigns, e-mail–borne malware, or Web site links to malicious sites.
- A botnet can also be used to instigate distributed denial of service (DDoS) attacks against Web sites or e-mail systems.
- Botnets can make huge amounts of money for terrorists and criminal organizations.

Gateway protection should also scan e-mail for sensitive, private, or confidential content. Powerful content and context analysis will help prevent data leakage, protect valuable assets, and ensure compliance with legal and regulatory requirements.

Content analysis scans the contents of a message for sensitive information controlled by a security policy. Content analysis engines need to be capable of scanning not only the text of an e-mail body, but also any attachments, compressed files, embedded objects, and password-protected documents.

Context analysis enforces policy-based compliance rules based on attributes such as the sender, destination, size of the e-mail, number of recipients, time, and header information.

Defend the e-mail server

Protection at the e-mail server has two benefits:

- ✓ Spam or malware for which protection may not have been available when it passed through the gateway can be stopped here.
- ✓ Internal threats sent between departments (not through the gateway) can be blocked.

Scanning interdepartmental e-mails for spam, malware, unwanted content, and sensitive information is critical. An employee might, for example, unwittingly visit an infected Web site and share the link with colleagues via e-mail, thereby placing more endpoint computers at risk of infection. Equally, while the H.R. department might need to share confidential information about staff members, such as salary increases for example, scanning of the e-mail server will ensure that this data is not inappropriately shared across the organization.

This level of defense will also protect message stores, ensuring that an organization's e-mail archives and those messages not yet downloaded to the local client remain free of malware.

Secure the endpoint

Endpoint protection should underpin an organization's security strategy, because it is the end user — and his or her confidential information — that is the ultimate target of many attacks. Cybercriminals attack the endpoint via numerous vectors, including Web sites, e-mail, instant messaging (IM), peer-to-peer (P2P) networks, and USB drives. Once infected, computers can be hijacked to spy on corporate networks, steal network resources, and unleash attacks on others.

Any endpoint defense also needs to take into account the different operating systems that are in use. Although the majority of business computers use Windows, a significant number of users operate Mac and Linux computers, and these are also at risk. Many attacks rely on the behavior of the user, not just the vulnerability of the operating system, making all operating systems more or less equally susceptible to security threats. This is why endpoint security requires protection for all major operating systems.

Control access to the network

Network access control (NAC) manages who and what connects to your organization's systems, protecting data and ensuring compliance with all regulatory requirements.

An effective NAC solution continuously assesses the computers of guests, employees who work out of the office, and unknown users against defined policies. It can verify, for example, that anti-malware and firewall applications are up to date, security patches are installed, and prohibited applications are not being used.

A preventive approach to NAC stops problems before they happen by combining pre- and post-connect assessment of computers with multiple remediation and enforcement options. NAC will allow you to quickly define endpoint security and acceptable use policies (AUPs) for all end-user scenarios so you can detect and fix managed endpoint vulnerabilities before infection, quarantine infected computers, and block unauthorized computers. We discuss NAC in greater detail later in this chapter.

Choosing the right solution

Every organization has a point at which enforcement and/or management adds too much expense or overhead, thereby offsetting the apparent benefits of security. Even for large organizations with dedicated IT security departments, the less time spent on day-to-day administration, the better. An effective security solution should be assessed against a wide-ranging set of criteria:

- ✓ High volumes of e-mail processing that can handle millions of messages per day
- ✓ A single scan that can identify spam, malware, data leakage, and all unnecessary applications
- ✓ Small and rapid updates with minimal footprint
- ✓ Directory services integration for simple and central enforcement of AUPs on an individual, workgroup, or departmental basis
- ✓ Powerful reports that deliver data on the integrity of the whole e-mail system
- ✓ A single, consolidated view of all e-mail traffic, even in multiple server environments
- ✓ Performance monitoring that automatically alerts the administrator if corrective action is required
- ✓ Managed appliances that can be remotely monitored and maintained by the vendor
- ✓ A single vendor for streamlined deployment, management, maintenance, and support.

Instant Messaging

Instant messaging (IM) applications are rampant in many organizations and pose a major security threat. Most users are completely unaware of the threat posed by instant messaging, lulled into a false sense of security by the seemingly "instant" and temporary nature of their messages. There is no inbox or outbox, therefore no apparent paper trail, and because many organizations fail to recognize or address the instant messaging threat, there is a lack of monitoring that further leads users to prefer this mode of communication for "private" and "confidential" communications. However, there is absolutely nothing private, confidential, or even temporary about instant messaging. IM, like most e-mails, are sent as plain text across the public Internet, exposing the contents of the message to anyone along its path. Log files and transcripts of conversations are held on servers and in device memory.

Finally, IM applications have become the most prevalent and preferred method for spreading malware, including viruses and "zombies" used to create extensive botnets. Malware spread in this manner often avoids gateway and server protection.

To effectively mitigate the risk associated with IM applications, organizations must first determine the business need (or lack thereof) for instant messaging in the IT environment, then address instant messaging in their acceptable use policies. If IM applications are banned, or otherwise controlled, application control and endpoint security solutions need to be deployed to enforce this policy.

Network Access Control (NAC)

During medieval times, castles were built to provide safety and security. The castle was normally built in a strategic location with towering walls surrounded by a moat. Battlements were positioned along the top of the wall with bastions at the corners. A heavily fortified and guarded entrance was secured by a drawbridge to control entry to (and departure from) the castle. These measures created a security perimeter, preventing hostile forces from freely roaming through the castle grounds and attacking its inhabitants. Breaching the perimeter and gaining entry to the castle was the key to victory for an attacking force. After getting inside, the castle defenses were relatively simple, and the attackers were free to burn and pillage. Hard and crunchy on the outside, soft and chewy in the middle!

Similarly, during "modern" medieval times — well, at least the last ten years or so, defending the corporate network simply meant erecting a firewall around an organization's IT assets and controlling access to the network by establishing just one route for inbound and outbound traffic. Employees and the computers they used were mostly office-based, and easily protected within this immovable perimeter from viruses, spyware, and other malware. It was even called the castle-and-moat approach; the castle being the office, the moat being the firewall.

However, technology and working practices have changed and this has had a significant impact on the IT perimeter. Organizations also demand increasing mobility from employees — who in turn require network access while off-site — and need to open up their IT systems to contractors and guests. As a result, network perimeters have dissolved and gaps in security have appeared, exposing that soft and chewy middle. Unfortunately, a drawbridge doesn't suffice for network security and data threats are much more sophisticated and prevalent than marauding bandits and the occasional fire-breathing dragon. Securing the perimeter is still critical, but it's not limited to the network boundary or a single point of entry. Instead, organizations must now understand and assess a wide range of Network Access Control (NAC) solutions and deployment options.

At the gateway

Although the network boundary is no longer as clearly defined as it once was, it is still important to secure any gateways that exist within the network. This includes deploying firewalls and intrusion detection/prevention systems. The security policies required for these devices to be effective have become increasingly important — and complex.

Although designed primarily to protect organizations against external threats, many gateway devices now include software modules for DLP and corporate compliance.

In the data path

In-line enforcement places a security appliance directly between the endpoint and the network. Data is unable to pass between the endpoint and the network without first being re-routed through the security appliance.

Data in motion (see Chapter 1) and other network traffic, including e-mails, instant messages, Web traffic, database transactions, and file transfers, is "sniffed" for sensitive content. In addition to monitoring and alerting, these tools can block content based on established policies.

On the network

Other network appliances are termed *out-of-band* — they do not reside in the data path but are on the sidelines, watching as traffic passes by. These appliances are called *post-connect* appliances because they only scan data packets after the endpoint has connected to the network and begins to send traffic. These appliances typically look for abnormal behavior patterns in the data sent from the endpoint to determine whether it is infected.

Endpoint Compliance

The most effective DLP solutions are integrated at the endpoint level, ensuring that the computer is automatically assessed before and during any connection to the network, at any time of day or night. Importantly, this allows organizations to easily ensure that an individual endpoint is in compliance with their security requirements before it joins and (if out of compliance) compromises the network.

Endpoint compliance solutions are entirely software-based. There is no impact on network processing speeds and it can easily be rolled out across an organization's existing complement of endpoint computers, plus any new devices as and when they are added to the network.

Endpoint compliance solutions are driven by centrally defined and managed security policies, which are able to cover every conceivable request and are easily updated.

Endpoint compliance policies can be as specific as an organization requires and are flexible enough to react to changing organizational requirements. New individuals, groups, or roles can quickly be added to ensure continued operational efficiency, while verification requests for the latest security patches can also be included.

Ensuring compliance

An unintended consequence of providing employees with company-issued endpoint devices is *configuration drift*. Many organizations grant individual users administrative rights over their laptop or PC as a way of reducing help desk requests and providing workers with greater flexibility. Over time, many users then change the configuration of their computers, thereby drifting away from the organization's security policy, until it is eventually out of compliance. Examples of configuration drift include disabling personal firewalls and installing instant messaging (IM) software — both of which cause significant security holes.

Endpoint compliance can identify whether a computer's configuration has been altered since it was last connected to the network, and then bring it back into compliance before access is granted. For example, firewalls are automatically switched back on and IM software is disabled.

Who and what wants access?

Endpoint compliance works with both managed and unmanaged devices, and both known and unknown users.

With a managed endpoint, organizations install an endpoint compliance agent directly onto the device, which communicates directly with the policy server. The agent is able to assess the device against the organization's security policy and request updates from the server if the policy has been changed.

When a user travels and is not connected to the corporate network, the endpoint compliance agent can stay in communication with the policy server over the Internet. If the policy server is not accessible, the agent uses the cached policy on the device's hard drive, ensuring that the endpoint remains consistent with the security policy and protected until it next connects to the network.

Device and user types

Managed device used by a known user. This is a company-issued computer in which the organization can dictate the software installed and the compliance policies.

Unmanaged device used by a known user. This is a guest — such as a contractor or consultant — who requires network access via the individual's own computer. The organization has no right to install software, but certain types of applications (such as antivirus) can be mandated without specifying a vendor.

Unmanaged device used by an unknown user. This is an access request from an unauthorized person attempting to access the organization's network from an unauthorized device.

Non-employees requiring network access through their own endpoint computers is increasingly common, with examples including auditors undertaking annual audits, contractors contributing to projects, and clients requiring Internet access.

Endpoint compliance deals with unmanaged computers by downloading a dissolvable agent to undertake pre-connection scanning. The device is checked to see

- The type of security application, vendor, and version number that is running (see Figure 6-1)
- Whether it has the latest operating system patches
- When it was last scanned for malware
- Whether its signature files are up-to-date

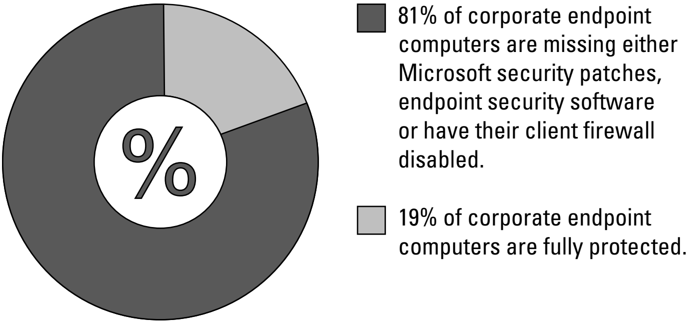

Figure 6-1: Are your endpoint computers a security risk?

Endpoint compliance allows organizations to:

- Identify who is requesting network access
- Assess whether the user's computer has the correct security requirements
- Grant or refuse a request, or quarantine a computer until it complies with security requirements
- Ensure that users only visit that part of the network that their role or task requires

Chapter 7

Ten (Okay, Six) Ways to Reduce Your Data Leak Risks

In This Chapter

- Encrypting, monitoring, and controlling your data and devices
- Covering the basics with anti-virus protection
- Implementing network access control (NAC) at the endpoint

In this chapter we take a look at some solutions you might consider to control data leakage within your organization.

The following areas are covered by many point-product solutions, so we recommend that when considering technology safeguards, you evaluate which products provide an integrated approach to the areas you wish to address.

Encryption

Implementing full-disk or file-level encryption is the best way to protect your organization's confidential information and comply with regulatory requirements.

Features to consider:

- Centralized data security control across mixed IT environments
- Consistent implementation and enforcement of company-wide security policies
- Reporting, auditing, and logging capabilities to monitor regulatory compliance
- Centralized key management making storage, exchange, and recovery of keys simple and easy to use
- Comprehensive data protection on all kinds of devices: laptops, desktops, removable media, PDAs, CDs, and so on

TIP

The Sophos solution for encryption is **SafeGuard Enterprise**.

Device Control

Controlling the movement of sensitive data needs to be a top priority for any organization seeking to reduce the risk of data leakage.

While a technology solution can provide pre-configured policies that will close the loopholes in the security defenses, it is imperative that user behavior is also addressed to ensure that employees are aware of both the value of the data to the organization and the repercussions of data being lost.

Features to consider:

- Comprehensive coverage of the ways in which sensitive data can be taken off computers and stored on portable devices — removable storage devices, CD/DVDs, smartphones/mobile devices
- Flexibility to authorize the use of some devices for certain employees based on roles and responsibility

TIP

Sophos solutions for device control include **Endpoint Security and Control** and **SafeGuard Enterprise**.

Data Monitoring

Data monitoring is critical to ensure an organization knows what data is leaving its network and systems, and what data needs to be restricted. To be able to do this, it is important to understand the various means by which sensitive data can be moved from the network and out of the organization — via e-mail, Web, instant messaging and removable storage.

Features to consider:

- Ability to automatically and consistently identify sensitive information in office documents
- Strong auditing and reporting, should the need for investigating the movement of sensitive data arise
- Flexibility to set a range of actions when the movement of sensitive data is detected, e.g. allow, block, or permit the user to decide if the movement is not transgressing the policy

TIP

The Sophos solutions for data monitoring include **Endpoint Security and Control, E-mail Security and Control,** and **Web Security and Control**.

Application Control

Unauthorized applications have the potential to create security, legal, support, and productivity issues. Users with local administration rights can download and install applications that may provide efficiency gains, but that may also cause less desirable results. User-installed applications (such as VoIP, IM, games, and P2P software) increase security and data leakage risks for your organization.

Features to consider:

- Automatic updating of application list when new versions of the applications are released
- Broad range of application types covered, from file sharing through to virtualization software
- Ability to block not just the installation but also the execution of unwanted applications

TIP

The Sophos solution for application control is **Endpoint Security and Control**.

Anti-Virus

Installing anti-virus software and keeping it up-to-date on all your organization's endpoints and servers remains a critical security practice for keeping your systems — and your information — safe.

With malware attacks becoming more targeted in an attempt to siphon data off computers, it is vital that you are protected against malware that tries to install software such as rootkits on your computers.

Features to consider:

- Complete defense against viruses, spyware, adware, rootkits and potentially unwanted applications across a wide range of platforms
- Protection against known and unknown threats through proactive analyzing of code before it runs
- Automatic enforcement of security policies when new computers join your network

TIP

The Sophos solution for anti-virus protection is **Endpoint Security and Control**.

Network Access Control

Having defined a security policy that covers the above points, organizations need to be sure that the policy is consistently and continually enforced across the network.

By assessing company computers that connect to the network, you can correct any changes that have been made to the computer by the user (such as disabling the anti-virus product) to put the computer back in line with policy. Guest computers that are given access to the network should also be assessed to eliminate any possible configuration issues that may present an opportunity for malware to attack.

By enforcing the policy, should a data breach occur, you can clearly show auditors that steps were undertaken to prevent the information from falling into the wrong hands — for example through enforcing disk encryption.

Features to consider:

- Ability to define security and acceptable-use policies and enforcement actions for as many distinct user groups as required
- Phased rollout of enforcement steps — from Report Only, through Remediation, to Enforce — avoiding an all-or-nothing approach
- Reporting that shows the overall compliance state of each user, including the compliance status of each application on the computer

The Sophos solutions for network access control include **Endpoint Security and Control** and **Endpoint Compliance and Control**.

About Sophos

Sophos enables enterprises all over the world to secure and control their IT infrastructure. Sophos's endpoint, e-mail, Web, and network access control (NAC) solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage, and compliance drift.

With more than 20 years of experience, Sophos's reliably engineered security solutions and services protect more than 100 million users in more than 150 countries. Recognized for its high level of customer satisfaction, award-winning channel program, and powerful yet easy-to-use solutions, Sophos has an enviable history of industry awards, reviews, and certifications.

Sophos is headquartered in Boston, MA and Oxford, UK and has offices in Italy, Germany, France, Singapore, Australia, Canada, and Japan. SophosLabs, the company's global network of threat analysis centers, which are located at four corners of the world, ensures that Sophos is able to respond to new threats without compromise regardless of time zone.

Sophos Endpoint Compliance and Control offers the only truly vendor neutral and software based solution for endpoint compliance assessment and network access control. Its preventive approach to pre- and post-connect assessment of computers helps companies to meet regulatory, industry, and internal compliance standards with policy enforcement and remediation. Sophos simplifies compliance policy creation, providing more than 1,000 predefined applications and operating system patches, and a simple-to-use interface allows administrators to change policy modes from reporting to remediate to enforce with one click of the mouse.

Sophos Endpoint Security and Control 8.0 include standard Sophos NAC functionality as well as comprehensive endpoint protection for complete protection against viruses, spyware and adware, and control VoIP, IM, P2P, and games.

www.sophos.com