Compliments of TREND MICRO

North American Small Business Edition

IT Security

FOR DUMMIES®

Learn to:

- **Protect your business**
- **Write a security policy**
- **Build a secure defense**
- **Combat the rising tide of threats**

Trend Micro Incorporated, a global leader in Internet content security and threat management, aims to create a world safe for the exchange of digital information for businesses and consumers. A pioneer in the antivirus market with over 20 years experience, Trend delivers top-ranked security that fits customer needs, stops new threats faster, and protects data in businesses of all sizes.

Worry-Free Business Security is a security solution that was built with a small, growing business in mind. It provides fast, effective, and simple protection against viruses, cybercriminals, and data loss, so you can focus on your business instead of worrying about Internet security

IT Security FOR DUMMIES®

NORTH AMERICAN SMALL BUSINESS EDITION

by Trend Micro

Wiley Publishing, Inc.

IT Security For Dummies®, North American Small Business Edition

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

Published by Wiley Publishing, Inc., Indianapolis, Indiana

ISBN: 978-1-118-08410-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Development Editor: Peter Gregory
Project Editor: Jennifer Bingham
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Custom Publishing Project Specialist: Michael Sullivan
Project Coordinator: Kristie Rees
Layout and Graphics: Melanee Habig

Table of Contents

Introduction

You've seen the effects of viruses, spam, and spyware on computers — infecting files, blocking up e-mail, and, in some cases, even killing off what might otherwise have been perfectly workable machines. But what's the impact of all this on a business? You have basic IT security measures in place, but are they enough? And if there's something sinister going on in your networks, are you able to detect it?

With businesses increasingly trying to do more with less and with funding tight, security may slip down a few notches on the priority list — you have so many other things to focus on! But with threats to your IT security coming from all sides, security is an increasingly necessary activity.

A small business is particularly susceptible to IT threats because it doesn't have dedicated IT staff keeping on top of security updates. But don't worry; it's probably easier than you think to protect yourself — and reading this book means you're taking the first steps toward that goal.

Simply put, investing time and effort in protecting your business helps you avoid cost and harm further down the line and safeguard future success. This book sets out some of the security basics for a small business owner, examines where the major threats are coming from today and in the future, and looks at some new solutions to the growing challenge of managing security.

Understanding the threats your business faces, their potential impact, and the regulations you need to follow is really the least any business owner should be doing. Going the extra step and writing up a security policy — and maybe even acceptable use policies for staff use of company email and Internet — is about protecting yourself even more.

About This Book

This book shows that investing in security doesn't have to be a particularly expensive or time-consuming business. In fact, you're probably already taking many of the necessary security measures; you just need to make sure your various tools and protections are working together. Investment in security doesn't have to be particularly onerous or expensive; in fact, it's getting easier and cheaper.

You read every day about the cybercriminals out to get everyone. Increasingly their focus isn't just big business, but smaller companies, too. Chances are, smaller companies don't have such strong defenses, and can't afford the top consultants to help tighten them up. But small and midsize companies rely on technology, too — take out their web server or steal their mailing list and they're in a lot of trouble. The good news is that it's getting easier to monitor and manage security. Plus, the integrated technical controls that vendors offer are getting more sophisticated and more rounded, and different options are emerging to make it more affordable for companies of all sizes.

This book was written for and with Trend Micro, with information supplied by them.

Icons Used in This Book

For Dummies uses icons in the margins to highlight specific information. The icons in this book are:

The information next to this bull's-eye is something you can put to use immediately.

This icon points out information to keep in mind as you explore the topic.

Especially dangerous practices get this scary-looking icon.

Chapter 1

Evaluating Security Threats

In This Chapter

- Discovering the type of IT threats a small business faces
- Gauging their potential impact on your business
- Prioritizing your biggest issues
- Seeing what regulations you need to follow
- Assessing the security industry's changing response

This chapter identifies the frequent offenders: the security threats that come back to bite businesses time and again. It also looks at the possible impact of these threats on your business — from network downtime to financial loss and damage to your reputation with partners and customers.

Without getting carried away with doom-mongering predictions of impending Information Technology (IT) meltdown, there are certain risks you need to be aware of and regulations you need to follow. Planning ahead for potential disaster means if it does come to pass you won't be flapping around in a panic.

Recognizing the Biggest Threats

Ever since computer systems and networks were introduced into small businesses in the 1980s, various threats have hammered at the security of those systems. Whether you're a glass-half-full type and you think these dangers have been overstated, or a conspiracy theorist who thinks they've been played down, what is certain is that they aren't going to go away.

The Verizon Business/United States Secret Service annual survey of data breach investigations found that 27 percent of all security incidents occur in companies with fewer than 100 employees. Twenty-seven percent may not seem like a lot, but if you have fewer than 50 employees and no dedicated IT staff, every security breach is not only a major pain, it can also be a huge drain on your resources.

Being savvy about the threats is the first step toward facing up to them. In these days of identity theft, spam and *spyware* (unwanted software on users' computers that secretly monitors their activity, with the intention of recording business and personal information and passing it on), you may be surprised at how fundamental some of the biggest threats are.

According to the Verizon/Secret Service survey, the most serious types of incidents experienced by U.S. businesses were the following, with the events ranked in order of frequency:

- Staff misuse of information systems
- Hacking and other attacks by outsiders
- Malware infection or disruptive software
- Social tactics aimed at exploiting employees through deception, manipulation, intimidation, and so on.
- Physical attacks like theft, tampering, and surveillance
- Errors, meaning anything not done or anything done incorrectly or inadvertently

There is another angle to these statistics. If we consider the amount of data compromised by an attack, malware and hacking account for over 90 percent of security breaches, whereas the other causes are each under 5 percent. So in terms of data loss — the most potent threats to businesses are malware and hacking attacks.

The Verizon Secret Service study stated that 86 percent of security breaches were compromises that took place on servers and PCs. An incredible 98 percent of data stolen was taken from servers. That tells us that PCs and servers need better protective measures than they're getting today.

A glossary of key threats

Knowing your backdoor from your bot is valuable knowledge in the realm of IT security, so check out the definitions in the following list:

- **Adware:** Software that displays advertising banners on web browsers such as Firefox, Internet Explorer, and Safari.
- **Backdoor:** Application that opens computers to access by remote systems.
- **Bot:** Remote-controlled *malware* that infects computers; a collection is known as a *botnet* that is controlled by a *bot herder* or *botmaster*.
- **Denial of Service (DoS) attack:** An attack that interrupts or inhibits the normal flow of data into and out of the system, ultimately rendering it useless. A DoS attack is any malware or action that stops the normal functioning of a system or network.
- **Drive-by:** a malware attack where attackers implant malware on a website; malware will be installed on the computers when users visit those infected sites.
- **Hacker:** a person or organization that develops or distributes malware or carries out attacks on target systems.
- **Keylogger:** *Spyware* that records and reports on keystrokes; often used to collect username and password information that is sent back to the keylogger's owner.
- **Malware:** Short for malicious software, it's any malicious or unexpected program or code, including viruses, Trojans, worms, bots, and spyware.
- **Pharming:** An attack on end-user workstations or IT servers that causes users' browsers to connect to hackers' imposter websites instead of the sites that users intend to visit. Often this is done with online banking and other high-value sites in order to steal login credentials from unsuspecting users.
- **Phishing:** Technique in which users are duped by legitimate-looking emails into handing over personal data to a bogus website.
- **Rootkit:** A collection of tools a hacker uses to mask intrusion and obtain access to a network or system in a way that is difficult to detect.
- **Spam:** Unsolicited junk email; can contain malicious code in attachments or links to malicious code stored elsewhere.
- **Spoofing:** Programming computers to impersonate others. IP spoofing uses a fake IP address to access a network.

(continued)

(continued)

- **Spyware:** Unwanted software that secretly monitors a user's activity, generally recording personal information and passing it on.
- **Trojan:** A type of *malware* that appears harmless, but has some hidden malicious intent.
- **Virus:** Code written with the intention of replicating itself. A virus attempts to spread from computer to computer by infecting other files.
- **Worm:** Type of *malware* that can spread copies of itself or its segments across networks.
- **Zero-day exploit:** *Malware* exploiting a newly discovered vulnerability in a system before a patch (fix) is made available.

And, before you get comfortable, thinking your business is safe from all these threats, we'll just point out the ever-changing nature of IT threats. In the past, malware and hacking attacks were mostly carried out by kids (security professionals call them "script kiddies") who were bored and needed something to do. But today, most break-ins are carried out by organized crime gangs and organizations that have deeper resources and are highly skilled. We offer advice on how to keep your system safe from these threats in Chapter 5.

As IT gets more sophisticated, don't forget to account for the fundamental threats. Staff misuse of systems is at the top of the current threat list. Perhaps, with the greater sophistication of security systems, some businesses are forgetting to lock the windows and doors.

Facing the Impact of Security Breaches

Security breaches can seriously hamper your business — from financial losses to damaging your business's reputation.

According to a Ponemon Institute study, the mean corporate loss to IT security breaches in 2009 was $3.8 million. In the study, companies that suffered a breach spent an average of $18,000 per day for as long as 14 days to remediate the breach.

The Digital Forensics Association also performed a study of more than 2,800 publicly disclosed security breaches over a five-year period. The average cost of a breach in that study was about $9 million.

These are pretty sobering figures. Often, a combination of repercussions from a breach creates even bigger problems. For a smaller company, the most serious issue may be business continuity or lost productivity. The direct financial damage plus the cost to remediate a breach can seriously threaten a smaller company's long-term viability.

Dependent as you are on IT today, the disruption to everyday running of the business can be catastrophic. Just consider the following scenarios:

- Your network has an outage, or the server isn't performing properly. What is the financial impact of each hour of lost productivity?
- Your website goes down and you lose a day's worth of orders. What's the damage going to be to your income and to your reputation?
- Your employees spend time surfing websites that are unrelated to your business, such as Facebook or Twitter. How much does this cost you in lost productivity, and what risks does it pose to your IT system?

Employees can directly damage your reputation by surfing content on the web they legally should not. Indirectly, their web browsing can threaten the business by bringing in malware that can infiltrate one of your PCs and install spyware or a *botnet* on computers that contain company data. This can cause the spyware or botnet to spread to more computers in your business and be very difficult to clean up afterwards.

According to the Verizon/Secret Service survey, the number of publicly disclosed breaches fell a little in 2009. However, it only takes one calamitous event to take your whole business down.

Consider the hidden impacts of security breaches. Often the most serious issues are the ones you don't immediately think of, such as the loss of a key piece of business information that you need to complete a deal, or the passing of data into a competitor or criminal's possession.

Check your insurance to make sure that you're insured against the financial losses related to a data security breach. Put disaster recovery and business continuity measures in place so that you can get back up and running in the shortest possible time after a security event.

The following sections lay out some of the impacts of security breaches.

Prompting PC, network, or website downtime

Almost all security incidents cause some form of downtime. A serious incident can take a PC, network or web server out of operation altogether. Even a less serious problem, such as a *denial of service attack* (an effort to prevent your customers and employees from accessing a system or network) can slow your network to a crawl.

Timing can be critical; if your PC is taken out of action when you're working on a pitch for a new piece of business, who's to say what the ultimate cost of that downtime is? Equally, if your website's not available when a customer wants to place an order or ask a question, that customer may never come back.

A slowdown tests the effectiveness of your contingency plans in full. With good disaster recovery or business continuity arrangements in place, you can restore lost data or switch to a redundant machine or network and continue working as if nothing has happened.

Dealing with data damage, destruction, or theft

You may not realize it, but most businesses are dependent on data to function properly. Like it or not, data oils the wheels of business — from the most basic customer names and addresses, to the fundamental intellectual property that makes your products and services unique, to the mundane administration of payments and invoices. Having that confidential data damaged, destroyed, or stolen can cause you lots of grief.

The theft of customer information can be highly damaging. How many times has a salesperson left a company taking its biggest clients with him? Or, in the case of intellectual property, how often has a company director left to start up another business, which ends up doing something remarkably similar to the one she left? Incomplete or missing data can be equally damaging, and its absence only tends to be realized after the fact, when it comes to enforcing contracts or dealing with company administration. Larger companies have safeguards in place to prevent this sort of thing happening; for smaller companies they're an all-too-common occurrence.

Data-stealing malware is, according to the latest research from TrendLabs, now one of the fastest growing categories of threat. It comes in several forms, and you may not even know that it's going on. The primary goal is to capture sensitive data from users' PCs and secretly send it back to criminal operators either for direct exploitation or resale on the black market.

It can be difficult to know if your data has been stolen, because usually it is still on your system and it is just a copy that has been stolen.

Recovering from identity and password theft

Everyone now knows the dangers of identity theft in the consumer environment, but you may not know that it's equally serious in the business arena. By stealing passwords and entry codes, fraudsters can pose as company officials.

Because company accounts usually run on credit terms, impostors posing as company directors can run up sizeable debts before being found out. Then when it comes to settling a bill at the end of the month, the company has a nasty surprise.

According to online security group Get Safe Online, corporate identity theft can take many forms including:

- Setting up a merchant account in your company's name and then accepting lots of purchases using stolen credit cards and depositing the receipts in the criminals' bank

account. By the time people complain and the credit card company comes to you for the chargebacks, the thieves have disappeared with the money.

- Rifling through rubbish bins to get employee names, bank account details, and other sensitive information.
- Ordering goods from your e-commerce site with stolen credit cards or by telephone with bogus account details (made to look like a real company).
- Hacking your website so it presents bogus or damaging information or hijacking it altogether to distribute porn or malware.
- Using data-stealing malware to collect the username and passwords to your online bank and transferring your funds to another account.

According to the 2010 Javelin Identity Fraud Survey Report, 11.1 million people in the U.S. alone were victims of identity fraud with a total cost of $54 billion, an increase of 37 percent since 2008. Identity theft is certainly a growth industry!

Facing financial theft

Reported financial theft from companies is actually quite rare. The UK-based 2008 Information Security Breaches Survey finds that no financial loss was incurred in 88 percent of the most serious breaches. Statistical data for the United States is almost certainly similar to this, as companies in the United States and the UK are not required to report *financial* theft to authorities. Most businesses handle these matters internally in order to avoid the public embarrassment of a public trial (the lack of controls would become a part of the public record).

But most attacks today are financially motivated, with some kind of financial pay-off the ultimate goal. So if it's not your company losing money, the chances are someone else will pay the price further down the line.

Accounting for the response costs

Orchestrating a response to a security incident can cost quite a bit, although you may find it difficult to measure all the expenses.

Some of the costs you may not immediately consider include:

- **Employee productivity:** As the biggest cost for most companies is people, the disruption to employee productivity is the biggest impact of any incident. That includes not just the time of the people who reinstall the operating systems and those who work to restore data, but also the cost of everyone who can't get on with their work while systems are being restored.
- **Lost opportunity:** Time is money in business, and the *lost opportunity cost* — the potential revenue that you could have been generating if you weren't recovering from an incident — is another factor to add in.

Taking a hit to your reputation

One of the great intangibles in quantifying the impact of a security breach is the damage it does to your business in the eyes of your customers. Customers and partners probably don't care that you were busy dealing with a security breach; they just know that you didn't provide the service they expect. Customers, partners, and investors may subsequently see you as a higher risk. In addition, your employees' attitudes toward what they see as unnecessary downtime can influence their commitment and productivity.

If a customer is having doubts about dealing with a smaller supplier, the occurrence of incidents will only confirm their suspicions that they should be dealing with a bigger player better able to prevent and handle such hits. This is particularly true if your business stores or processes any sensitive information about your customers' employees or customers.

Assessing the Threat to Your Business

Clearly the importance of information security threats differs from one business to another. For a high-tech start-up with lots of digital assets, the challenge is about protecting its networks and systems and managing its reputation and relationship with suppliers and buyers. For a more traditional firm, such as a taxi company, IT security is more about managing and protecting the PCs and servers in its network, applications, and communications infrastructure.

Some threats are universal: The physical theft of computer equipment affects any business as it spends money replacing the stolen goods. But it's worth thinking about the specific vulnerabilities that your business has and what threats might affect you. Use Figure 1-1 to run through the major threats listed across the top and check off vulnerabilities your company faces from the list that runs down the side (the ticks represent areas where the major threats could have an impact).

Doing a formal risk assessment, in which a third party independently looks over the vulnerable points in your IT environment and outlines the risks you could face, is a valuable exercise. Some vendors conduct such a study for a nominal fee. Every company is different, so it's worth having an expert conduct a tailor-made risk assessment; you might be surprised at the results.

	Systems Failure	Virus/Malware Infection	Staff Misuse	Unauthorized Access	Physical Theft	Computer Theft	Information Theft
Website	✓	✓		✓	✓		
Confidential Data				✓	✓		✓
Critical Comms Infrastructure	✓				✓		
Mission Critical processing	✓	✓	✓	✓	✓	✓	✓
E-mail Comms	✓						
Other							

Figure 1-1: Checking vulnerabilities and threats.

Looking at Legal Responsibilities

You need to bear in mind a range of legislation when considering your IT security responsibilities. Principally, your organization needs to consider your privacy and electronic communication responsibilities and your treatment of staff, as well as keeping in mind a plethora of state and federal laws and regulations.

Respecting privacy and communication

The Electronic Communications Privacy Act (ECPA) of 1986 prohibits eavesdropping on telephone, email, and electronic communications unless a search warrant is in place.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires organizations that store any health-related information have many specific safeguards in place to protect Electronic Patient Health Information (EPHI) from unauthorized access and loss.

The Gramm-Leach-Bliley Act (GLBA) of 1999 requires financial institutions to develop and disclose privacy policies to their customers, and to protect customers' private information from unauthorized access.

The Fair Credit Reporting Act (FCRA) of 1970 allows U.S. citizens to opt out of unwanted solicitations of credit. The Fair Debt Collection Practices Act of 1978 limits the dissemination of information about consumers' financial transactions. The Fair and Accurate Credit Transactions Act (FACTA) of 2003 was put in place to help identity theft prevention and other measures for financial institutions and creditors.

Many U.S. states have data privacy laws that require an organization that has suffered a security breach of citizens' sensitive data to disclose the breach to affected citizens. Some of these state laws require companies that suffer security breaches to publicly announce the breach if they can't precisely determine which citizens' private data has been compromised.

The U.S. Federal Trade Commission has taken an active role in the enforcement of companies' online privacy policies.

Companies that conduct business online are expected to do what their privacy policies say they do. Companies that do otherwise face heavy fines.

The Telephone Consumer Protection Act and the Junk Fax Prevention Act place restrictions on your ability to perform telephone and fax business solicitation. Private citizens can add their phone numbers to a national "do not call" registry that places those citizens off-limits for unsolicited calls.

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 makes most unsolicited commercial emails illegal.

The Identity Theft and Assumption Deterrence Act of 2003 makes it illegal to possess any "means of identification" used to commit fraud.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) restricts the collection, storage, and use of citizens' private information.

Treating staff lawfully

A whole host of regulations covers companies' responsibilities toward their employees, including:

- Computer Fraud and Abuse Act of 1984.
- Computer Security Act of 1987.
- Many U.S. states have laws protecting citizens by requiring businesses to inform them of security breaches of citizens' private data. These laws apply to your employees.
- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 as it applies to your own employees' health-related information.

Businesses also need to be careful regarding the examination of its employees' email messages. Several court opinions have come down on either side of this issue. Businesses that have clear policies stating that any email sent or received on company owned computers is company property have a better leg to stand on here.

Generally speaking, organizations should put measures in place to protect all internal information from unwanted disclosure or compromise.

The Security Industry's Response

Early in the evolution of IT security, vendors concentrated on one area of IT security, such as antivirus software or firewalls, at the expense of others. But the industry's response is now beginning to expand, as companies realize they need a coordinated defense against information security attacks.

Firewalls and anti-malware technology have become more sophisticated and have been bundled into suites with other capabilities, including anti-spam and anti-spyware technology. *Endpoint security*, which focuses exclusively on the PC or other device at the user end, is being augmented with some of the capabilities of *gateway security* (security placed in front of the Internet connection) specifically to block web threats before they reach their intended target. The new trend is toward layering protection across both the gateway and the endpoint.

The emergence of hosted security services is another welcome development for small businesses. This reduces IT overhead, both in terms of hardware cost and management, and it's more reliable, as elements of the security solution are housed on the security provider's servers. We discuss these further in the next chapter.

You may think you need to have security services running onsite, but many companies already use hosted services in the form of webmail, customer relationship management (CRM) software, and may even have an outside service provider running their payroll. Using a hosted security service really makes a lot of sense — the guys who develop the software are the most qualified to run it for you, and they've got processing capabilities the likes of which you could only dream of.

The pay-as-you-go model also provides a predictable monthly or annual cost on your balance sheet without you having to worry about the cost of future upgrades as IT security continues to evolve.

Chapter 2

Starting with a Security Policy

In This Chapter

- Understanding the need for a security policy
- Looking at standards and best practice
- Dealing with administering security
- Implementing technical controls

After you recognize the threats and sign up to the principles of good IT security (see Chapter 1) your next question may well be: Where do I start? If you've already looked at the risks your kind of business is exposed to, the first step is to develop a security policy for your company and communicate it to staff.

Next, you consider how you're going to enforce the policy, including the technology you already have in place to police security risks and any gaps you might need to plug. Technology is only part of the picture though — it's also about people, processes, and policies.

This chapter also takes a peek at the sort of best practice businesses might use and asks what, if anything, it can teach us.

Formulating a Security Policy

A company security policy is the foundation on which good IT security is built. A *security policy* is a statement of intent for how you plan to protect your digital assets and police your

organization. It acts as a central repository of guidance for management, staff, and third parties and includes everything from processes and procedures, through people's roles and responsibilities to a description of the technical measures you have in place and how you will recover in the event of an incident.

You base your security policy on the risk analysis outlined in the previous chapter and on an awareness of the most serious threats you face.

To make sure it has authority, a security policy should be approved by senior management and reviewed from time to time, and as circumstances change. No need to go into great detail on every point, but look on the security policy as a plan of action, outlining what the company's critical information assets are and how it intends to protect them.

It's best if you can take a layered approach to putting the security policy together, starting with a high-level mission statement, and then moving down deeper into physical devices, roles and responsibilities of staff, including references to acceptable use, how breaches will be dealt with, and so on. This is also a good place to house your business continuity and disaster recovery plans.

Sorting out what to include

Security policies differ from one company to the next, but, at its most basic, any policy should include the following:

- A clear explanation on the purpose of the policy, including the ultimate goals and strategic importance of information security to the business.
- A statement of support from senior management, demonstrating their commitment to information security.
- The training available to help employees understand information security and risks.
- An explanation of minimum security standards, with an emphasis on procedures to follow in areas that are of particular importance to the business. For example, every security policy should outline elementary precautions concerning computer viruses, guidelines for how to

behave on the web and instructions for setting up passwords.

- Definitions of roles and responsibilities within the business for information security.
- The requirement for reporting, responding to, and resolving security incidents.
- The need for business continuity plans, which explain how the business will continue running in the event of catastrophic failure such as fire or flood.
- References to supporting documentation, such as staff policies, procedures, guidelines, or security specifications and standards. For example, if you want to go into more detail on Internet policy, you might include:
    - The company's use of the Internet and the related threats
    - The Internet services that can be used and those that are off limits
    - Who authorizes Internet connections
    - Who is the single point of contact responsible for the IT security policy (although everyone is responsible for implementing that policy, of course)
    - The standards, guidelines, and practices to be followed

One of the weakest links in a company's security chain is often password protection, as users tend to jot down their passwords on a sticky note next to the machine or leave the default password on. Make sure that your security policy warns against this type of risky behavior and establishes safe protocols for password quality and protection.

Going further, you might want to set up an *acceptable use policy* as part of the security policy, which outlines what the company deems to be in and out of bounds. We cover this in the next section.

You may want to introduce a separate acceptable use policy for Internet access, for company email, remote access, telework, mobile devices (smartphones), and indeed for the use of any other company IT asset. We talk about acceptable use policies in the next section.

Don't get too prescriptive about policies and procedures for individual IT assets. The important goal of your security policy is to make staff aware of the policy objectives, why particular measures are in place and what the consequences are of breaking them.

A good rule of thumb for security policies is to state what must be done, but not how it should be done. Procedures and standards, which should be separate documents, describe how policies should be carried out.

Defining acceptable use

Protecting your IT assets starts with a staff that receives clearly communicated policies and guidelines on acceptable use, confidentiality and standards for security measures. An *acceptable use policy* spells out what is and is not allowed on company time and on company computers and explains the repercussions for disregarding the policy.

Without clear guidelines, employees may be exposing the company to malware, sharing confidential information over the Internet, or taking sensitive information off-site on laptops or USB sticks. And they also may be wasting company time!

Acceptable use policies may appear draconian to some, but as long as they strike a balance between pragmatism and control, and the company is clear about the risks it is trying to avoid, staff will understand their importance. You can even include employees in the design of the policies, gaining buy-in from day one, and encourage them to offer feedback on whether particular restrictions work — or not.

Tying acceptable use policies into employee contracts and disciplinary procedures helps weld them into the culture of the company.

As far as acceptable use policy goes, senior management should lead by example and follow this policy.

Browsing the Internet without putting the company at risk

Your employees need to use the Internet to do their jobs, but distractions on the Internet can and do decrease productivity and expose your company to threats from the web.

Suggestions of what to include in an Internet policy follow:

- The times when private Internet use is acceptable and not acceptable. For example, you might not want employees going on Facebook during working hours, and you might not allow friend requests to be accepted or rejected from the work computer.
- What kinds of material are off limits — porn, obscenity, racial hatred content, and so on.
- How to treat business confidential information — don't share it outside of the company's private network, for example.
- Suggestions for care of company property, such as laptops.
- Guidelines about downloading and installing software.
- Security guidelines, such as browser security settings.
- A ban on sharing and downloading copyrighted material.
- Details of any monitoring activity the company has in place.
- The consequences of breaching the policy.

A website filtering program can help prevent or detect some of the problems associated with Internet access.

Template for an acceptable use policy

The text here (adapted from a sample policy on `first.org`) sets out an acceptable use policy for Internet use. You can copy it and adapt it to suit your needs.

General Requirements

You are responsible for exercising good judgment regarding appropriate use of [Company name] resources in accordance with [Company name] policies, standards, and guidelines. [Company name] resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the [Company name] network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other

(continued)

(continued)

blocking technologies must permit access to the scan sources.

System Accounts

You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

You must maintain system-level and user-level passwords in accordance with the Password Policy.

You must ensure through legal or technical means that proprietary information remains within the control of [Company name] at all times. Conducting [Company name] business that results in the storage of proprietary information on personal or non-[Company name] controlled environments, including devices maintained by a third party with whom [Company name] does not have a contractual agreement, is prohibited. This specifically prohibits the use of an email account that is not provided by [Company name], or its customer and partners, for company business.

Computing Assets

You are responsible for ensuring the protection of assigned [Company Name] assets that includes the use of computer cable locks and other security devices. Laptops left at [Company Name] overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of [Company Name] assets to the [Name of appropriate group].

All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to ten minutes or less. You must lock the screen or log off when the device is unattended.

Devices that connect to the [Company Name] network must comply with the Minimum Access Policy.

Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, [device management or security system software name], [device management or security system software name], and [device management or security system software name].

Network Use

You are responsible for the security and appropriate use of [Company Name] network resources under your control. Using [Company Name] resources for the following is strictly prohibited:

Causing a security breach to either [Company Name] or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

Causing a disruption of service to either [Company Name] or other network resources, including, but

not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

Introducing honeypots, honeynets, or similar technology on the [Company Name] network.

Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. See the [Name of company document that details copyright restrictions] for additional information on copyright restrictions.

Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws. See the [Name of company document that details export restrictions] for additional information on export and transfer restrictions.

Use of the Internet or [Company Name] network that violates the [Name of appropriate policy], [Company Name] policies, or local laws.

Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, email bombs, spyware, adware, and keyloggers.

Port scanning or security scanning on a production network unless authorized in advance by Information Security.

Electronic Communications

The following are strictly prohibited:

Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates [Company Name] policies against harassment or the safeguarding of confidential or proprietary information.

Sending spam via email, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Use of a [Company Name] email or IP address to engage in conduct that violates [Company Name] policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a [Company Name] email or IP address represents [Company Name] to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

Policy on sending email

Email has become the prime method of business communication, so you need to make employees aware of safety procedures — and make sure they follow them. Some issues to address are:

- Using a disclaimer on emails ("this email is private and does not represent the views of the employer . . .").
- Guidelines on the opening and viewing of attachments received by email.
- Additional guidelines, if appropriate, relating to email applicable laws and to any anti-harassment policies that may be in place.
- How to handle confidential information sent by email and where you require encryption of email in accordance with company guidelines or state laws. For example, Massachusetts and Nevada require all personal info to be encrypted before being emailed.

Ensuring the policy works

Too many security policies collect dust on a shelf or sit on a computer hard drive neglected and unloved and, crucially, not enforced. For a security policy to be meaningful, it needs to be a living, breathing document that management and staff refer to and follow.

Combine an ongoing effort to make employees aware of and educated on the security policy with upper management's visible commitment to taking the policy seriously and ensuring that it remains relevant and up to date.

Social etiquette on acceptable use can easily change over time, while the type of Internet services available also mature and change, so build in a periodic review of your security policy to keep it relevant — a policy document based on an Internet browser no longer in use makes the whole document less effective.

Exploring Best Standards and Practices

The ISO standard ISO/IEC 27001 represents the gold standard for information security management. Developed from the British Standards Institute's BS7799-2:2002, following the standard gives you the benefit of years of developing thinking and practical experience on how best to set up and manage an information security management system. For more information, visit `www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/`.

Certification of your company's management system to the standard is probably too onerous for most small businesses, unless you are in a sector where you're keen to prove your information security credentials to customers or suppliers. But everyone can benefit from the standard's requirements, many of which are covered in this book.

If you're looking for help on framing a policy and IT security setup, you can find a lot of information and advice from several industry groups and security vendors, such as those in the sidebar "Getting more help."

Getting more help

- The SANS Institute (`www.sans.org/security-resources/policies/`) has many policy document templates.
- Forum of Incident Response and Security Teams (`www.first.org`) has many best-practice documents.
- The National Institute for Standards and Technology (NIST) (`http://csrc.nist.gov/groups/SMA/fasp/`) has a collection of federal agency security practices.
- Trend Micro (`www.trendmicro.com`) has a variety of further information resources available.

Administering the Security Policy

After laying down the company's security policy, based on a risk assessment of the kind of threats you face, you need to determine how to administer security. This comes down to a mixture of people, policies, processes, and technology, with each playing a critical part in ensuring overall security.

The more client machines your business has and the more complex your network setup, the more difficult IT security becomes. Having said that, most smaller businesses don't require additional staff to manage IT security systems, but often assign security responsibility to existing managers.

If you use an external consultant to set up the security system, make sure that the consultant reports back through existing management— don't leave it to an outsider to keep you safe.

Expect an IT security consultant to set up an *asset register* that lists all the IT assets the company has — from PCs to routers to external hard drives — and records the standards and procedures the company uses to keep them as secure as possible. The asset register becomes an important point of record when you make changes to the components of your IT environment. If you do suffer an incident, the asset register can help you find the root cause of the problem.

Forward planning is essential in setting up an information security system — imagining the worst-case scenarios and how your business might respond and recover from them. It's also much easier to plan for an incident before it's happened than when you're in the midst of a meltdown, struggling to access the right resources or restore systems so staff can start work again.

Exploring the Role of Technical Controls

The role of technology begins with the IT assets you have identified, then moves onto the protection systems you need to put into place.

To understand the issues related to designing effective IT protection and recovery systems, consider the following questions:

- Who will be responsible for ensuring systems are kept up to date and patches are applied to guard against attacks?
- Who looks after licensing of the software you use?
- How do you manage the backup of data? Make sure that you have separation of duties, so all the onus doesn't fall on one person and you are still secure if they are off sick or on vacation.
- How do you control access to IT equipment and data?
- How do you ensure staff members follow your policies on, for example, surfing the Internet — do you rely on them to be honest and follow the rules? Or do you put in place suitable filtering technologies?
- Do you have a process for making sure changes to IT hardware and software don't downgrade the security policies already in place?
- Do you have a disaster recovery plan? What measures do you have in place to recover from a serious incident such as a fire or network outage?
- What's your policy on employees using their own IT equipment for business purposes?

Some of the questions in the preceding list can be addressed with automated solutions, which lightens the administrative load for employees. For example, you can use identity management to safeguard access control, handing out security tokens to staff logging on to the corporate network. You'll probably have spam filters set up on your email. Anti-malware updates will almost certainly be automated to some extent, too.

You can lock down particularly sensitive areas of your IT architecture with firewalls. Your business continuity plans might include automatic backup to a secure online data store. And you might want to consider automatic encryption of data whenever it leaves the building. You may also want to implement a URL or website filtering solution to allow staff access only to websites that are appropriate to the work they undertake, not only reducing the risks of security breaches, but also increasing staff productivity — if they can't get to Facebook, they can't spend company time updating their profiles.

Outsourcing Security Functions — The Cloud Option

Administering security should not, at the end of the day, be a technical task. That's where cloud services (external hosting) comes into play; where the IT service provider runs the software on its own servers on behalf of the customer, who accesses it through the Internet. Cloud security isn't appropriate in all areas, but it works very well in two, which we explore in the next sections.

Cloud-based email security

Protecting the organization against spam is an obvious way to ease the administration overhead.

Up to 95 percent of email on the Internet is spam, and dealing with it eats up staff time, decreases productivity, and takes up network bandwidth and storage space. Spam is also a popular method of distributing malware, whether through phishing emails with links to compromised websites or by including unsafe attachments.

Cloud-based email security cleans email before it even reaches the network, reclaiming IT staff and end-user time and hardware and network resources. It frees up your bandwidth and reduces the impact on the mail server, as spam never arrives at the company in the first place.

A word of caution on cloud-based email security. The only thing worse than trying to retrieve an email that your filter has incorrectly specified as spam is not realizing that you were sent that email in the first place — it may have been something important like a piece of new business. You need to make sure that the cloud email security provider you choose has a good (low) record on what the industry calls *false positives* — emails it thinks are spam, but in fact aren't. The supplier might even offer a service level agreement based around low false positives, so you can make a financial claim should the false positive rate be over the agreed limit.

Cloud-based endpoint security

Another area where cloud-based security can really benefit a business is in managing the administration of endpoint security — the protection for the multiple PCs, laptops, file servers, and other devices your users have. Many of these are set up with the consumer-focused security products that they came preinstalled with. But not only are these products designed for home users, without the sort of features you'd want in a business environment, they also need managing separately.

That means different expiration dates, licenses, and configuration settings, leaving your systems admin person needing to master several different products and stumble through different configurations. More importantly, it means inconsistent protection from one machine to the next. In some cases, users might be administering their own desktop products and switching off essential updates, leaving your company unnecessarily exposed to threats. And when they take their laptops out of the office, security administration is completely out of your hands.

A good solution to this administrative nightmare — particularly for smaller companies — is to switch to a cloud-based offering. It's easy to set up on multiple machines, with users able to just click on a link and download the protection for their machine that works inside and out of the office. You don't have to maintain a security server, and everyone has consistent, business-class protection.

This type of solution also gives you a central management view through a console hosted on the Internet that provides visibility into what each machine's state is, what threats have been detected, and so on.

Chapter 3

Establishing a Coordinated Defense

In This Chapter

- Devising security systems to protect your systems
- Focusing some thought on physical protection
- Educating employees

Strong security isn't about one particular technology or discipline; it's a combination of measures that keep your systems safe from attack. Some of these you probably have had in place for many years, others might be new to you. But they are all equally important details that make up an overall picture of protection.

Many businesses lack a coordinated defense against security threats, with integrated technical controls that help enforce what you've agreed to at a high level. You may have super strong protection in some areas — such as a company firewall that blocks anything remotely suspicious from entering or leaving the company. In other areas users are protected by consumer solutions, such as the antivirus software that came pre-installed on your machines. But unless that's all coordinated with, for example, controls about who can override firewall settings and a central security management console (possibly in the case of a small business, hosted by their IT support provider), your uncoordinated security measures can give you a false sense of security and leave your environment open to attack and compromise.

This chapter outlines each of the areas in a little more detail. We're not aiming to provide an exhaustive explanation of any

one part, but instead to provide an overview and an understanding of how they all fit together.

Controlling Access

Access control systems ensure that the users who are allowed access to your systems are who they say they are, have permission to do what they are doing, can't infect your systems with viruses and other malware, and can't steal or gain access to information they should not have. Access tools include systems for authentication, identity management, permissions, user names, and passwords.

Without access control it's really easy for a hacker to force their way into an organization — but, unless you're a high-value commodities trading company, you don't need to go overboard about it.

Shoring up the perimeter

IT and business managers spend huge amounts of time and effort erecting the IT equivalent of huge fences around their systems. They buy firewalls and intrusion prevention systems and, in some cases, set up virtual private networks so users can securely connect to corporate systems when they're out of the office.

But hardening the perimeter is only the outermost defense — and no IT perimeter is impermeable. There are always holes in these fences, such as the HTTP (80) port a web server uses.

Checking ID at the gate

If you build elaborate defenses, such as firewalls and the like, you have to make very sure that the people you do let in aren't villains in disguise.

This is where access control comes in — it's the equivalent of shouting "Who goes there?" before you lower the drawbridge.

Choosing and maintaining good passwords

Because user names and passwords are the most fundamental level of IT security, it's important that you encourage everyone in the company to choose passwords that are difficult to crack. The following list shows characteristics of hard-to-crack passwords:

- A combination of upper and lower case letters and numbers
- Eight characters or longer
- Not composed of words or numbers that other people could guess easily, such as a spouse's or child's name

You also need to make sure that everyone takes care of their passwords. Basic password hygiene includes:

- Don't write down passwords or leave prompts near the machine used for access.
- Never leave factory default settings on — using the word "password" or "welcome" as a password is too easy to crack.
- Never give your password to a third party — even someone from your company.

Access control doesn't have to consist of complicated biometrics, such as iris scanning and fingerprints, although these methods are becoming more mainstream for larger companies. Most small firms, however, can take a more pragmatic — and affordable — approach to identity management.

Today, user names and passwords are the keys that open the IT kingdom and permit access to business information. You need both before you get on the machine you want to use, another to get on the company network, another for particular applications such as the accounts system, and maybe even another for a sensitive area of the company's data. That's access control.

Of course, you still need to ensure that if a person's accessing from outside the company they haven't got hold of someone else's user name. Even someone inside the company may try to look at something they shouldn't — such as the boss's salary and benefits.

Authenticating a user's identity is commonly based on four factors:

- Something they know — a password or PIN (personal identification number)
- Something they have — a smart card or security token
- Something they are — a person with a scannable fingerprint or iris
- A known location — inside the company's building

A company's protection is considered pretty good if every user can pass two of these four tests — after all, your bank trusts you to withdraw money with a card and your PIN. Requiring three of the four means your system is almost bullet proof.

Restricting actions

After being identified and authenticated, users may need to seek another stage of authorization to determine what actions they can take — are they allowed to edit files or just view them, for example.

In a business, you may want to set access up based on *roles* in the same way that you would in signing off expenses, for example. If you're the human resources (HR) manager you can view and edit employee details; if you're just an employee in the HR department you can view files, but can't change them.

When the HR manager goes off on holiday, or someone else takes on their role, that person assumes the same access rights to the HR records.

Employees who don't work in HR should not be able to access any of this data at all.

Securing Your Phones and Networks

Network, or gateway, security is the subject of much debate, but what some businesses don't consider is that they don't

just have one network to protect, they have many. Along with the Internet network, there's the phone network, an intranet, and sometimes an extranet network. There's probably a wireless network, and possibly a virtual private network (VPN), or some other method to allow remote workers to access the internal IT environment.

Each network probably has some measure of security attached to it — but is it the right level? It's the interconnectedness of these different networks that complicates the picture. If your network connection goes down, for example, in the past you might have picked up the phone and carried on working that way — but if you've got a VoIP (*voice-over-Internet protocol*) system, which runs the telephone service through your Internet connection, that may go down as well.

Ringing around telephone networks

Plain old telephone systems (POTS) and, in particular, private branch exchanges (PBXs) have always been the subject of hacking attacks and at risk of wiretapping. But few criminals had the technology or expertise to orchestrate such attacks.

Today, however, many businesses are switching their phone networks over to VoIP, eager to embrace the significant savings to be made on the phone bill and the ability to share the same network as the data network, resulting in lower infrastructure costs and management.

VoIP is more easily hacked or disrupted, because it runs on the same network as computer systems, so VoIP systems may be open to:

- **Fraud:** A cybercriminal hacks into your VoIP systems and makes lots of calls to premium rate numbers and you're left paying the bill.
- **Denial of service (DoS) attacks:** As with DoS attacks on Internet sites, a cybercriminal attempts to take down your phone service and prevent anyone else from using it.
- **Spam and phishing attacks:** Again, similar to computer systems, voice-synthesized computers constantly phone

lots of numbers in the hope that someone picks up the phone and is either duped into making a fraudulent purchase or wastes time dealing with a phoney call.

The fact that you're dealing with Internet protocols means you can adopt the same protection as you would for computer systems. However, consider the risk attached to the phone going down and whether you want to isolate your VoIP system from the rest of your IT environment.

Guarding wireless networks

In the first generation of wireless connections, users were very careless about enabling the security on routers and access points, partly because it was described as complicated, but also because people weren't aware of the risks.

Today, you need to know that wireless connections carry their own, unique security risks. These fall into a range of categories:

- **Piggybacking:** Other users jump on your connection to access the Internet, affecting performance and having full access to the network and its resources. This happens when no authentication or encryption has been enabled.
- **Session stealing:** On wireless networks with inadequate security, intruders on the same network can steal other users' website sessions. New tools such as "firesheep" make this practice easy for even non-technical intruders.
- **MAC spoofing:** Hackers get the MAC (Media Access Control) address of your network and use it to gain access and intercept network traffic.
- **Denial of service attack:** A cybercriminal prevents legitimate users from accessing the wireless network.
- **Man-in-the-middle attack:** A hacker sets up a bogus access point from which they can read all your traffic and insert phony, albeit real-seeming communications.

An older standard in wireless security has now been replaced with Wi-Fi Protected Access (WPA and WPA2), so as long as you set it up with secure passwords and keep them safe, the network connections you make should be pretty safe. WPA

and WPA2 authenticate users to check that they're allowed access as well as encrypting the data transmitted between the user and the network. Other measures you will want to incorporate include:

- Change your wireless network SSID to something that will not associate the network ID with your business.
- Turn off SSID broadcast.
- Incorporate network-based authentication if your wireless network supports this.
- Consider connecting your wireless network to the Internet only, and require users to connect to your VPN to access the internal network.

Even better, equipment manufacturers have made this security protocol really easy to set up, so you just follow a few simple steps and your wireless network is secured.

Protecting computer networks

Small business computer networks have always been open to attack — and security measures are generally pretty effective. According to some estimates, 80 to 90 percent of all businesses have invested in firewalls, and 50 to 60 percent in intrusion detection and prevention systems. The inclusion of these technologies in Microsoft operating systems has increased that number even further.

A *firewall* prevents unauthorized access to the network, but an *intrusion detection/prevention system* (IDPS) monitors network activity looking for malicious or anomalous behavior and reacting to stop it.

The trouble with computer security technologies is that when you lock down your computer systems so that your business is completely secure, and take every alert to be a hack attempt, you can prevent the business from functioning normally. Go too far the other way and it's almost pointless having this technology in place. The trick is largely a matter of getting used to the capabilities of the technology — and manufacturers of these products are making things simpler for network administrators.

Increasingly, network firewalls and IDPS are bundled together with other capabilities on a unified threat management (UTM) device. These are often hardware-based, self-contained units that a small business can almost literally buy, plug in, and leave in the corner to do its thing: facilitating access and protecting the network.

A company with remote users wanting to connect into the office network or a business looking to connect satellite offices to a main network may set up a *virtual private network (VPN)*, a technology that uses different methods to establish a secure connection. Using a variety of security protocols — usually Internet Protocol Security (IPSEC) for site to site and Secure Sockets Layer (SSL) for remote users' access — a VPN can be thought of as highly secure communication "tunnel" that automatically encrypts all data that passes through it.

You need to put some thought into how to set up user connections and how to authenticate users to a VPN. What happens, for example, if a user leaves their laptop on a train? Could a stranger pick up the computer and gain access to your company network?

Managing Security Management

Much of what constitutes IT security is about basic IT administration — making sure that you do the core housekeeping tasks that the business IT environment requires. Some of those tasks include ensuring that software is up to date and patches are applied — an important discipline as more and more vulnerabilities are discovered in different systems and software.

Avoiding zero-day attacks

Zero-day security attacks, which exploit vulnerabilities in software systems before the vendor can distribute a patch, are on the rise. Internet browsers have become a favorite point of attack, because they cover such a large volume of users and can be exploited directly as soon as a user arrives at an infected website. Microsoft's policy of issuing updates once a month on Patch Tuesday gives cybercriminals an entire month to exploit a vulnerability before a fix is issued.

Beyond good housekeeping, there's not a lot managers can do to protect against zero-day attacks, although proactively staying on top of major vulnerabilities and threats, and taking interim action to patch problems helps.

Much of the administration of security can now be automated, including patching through *Microsoft Update*, Microsoft's automated service for ensuring its software is up to date, automatically updating virus and spyware databases. You can even enforce some of the rules contained in your security policy by, for example, blocking access to certain applications to certain types of users.

Restricting user access

You can also include restrictions in your Internet usage policy that says, for example, no access to social media sites during the working hours of 9 to 1 and 2 to 6. We offer a sample acceptable use policy in Chapter 2. But how do you enforce that? You can't patrol the office spying on what people are viewing. URL filtering, with a high level of flexibility and categorization of different websites, can block access to inappropriate content according to a policy you set up, potentially saving hours in lost productivity.

The security policy also contains the information on roles and responsibilities — a housekeeping chore if you will. In a small business, this is rarely someone's first job, so ensuring that the job is being carried out as specified is important.

Overseeing the technology

Security administration also includes overseeing anti-malware (antivirus and anti-spyware) and anti-spam technology. Anti-malware has a very high penetration in large and small businesses alike, with upwards of 95 percent adopting it. It's also a very mature technology, with little to differentiate the leading products.

Today's edge comes in the administration of anti-malware protections with features that include:

- Keeping the databases of security updates offsite to reduce the load on the company's systems, plus

cloud-based solutions for email and endpoint security. More on this in Chapter 5.

- Having the computer automatically match potential threats with the threats in the offsite database.
- Central rollout of systems and upgrades without having to visit every desktop.
- Centralized management and reporting.
- Improved compatibility with older operating systems and hardware.
- Automated removal/quarantine of malware and accurate reporting/monitoring to system administrators.

Much malware infection comes from users downloading software, either knowingly or in ignorance — for example, being duped into upgrading to a more up-to-date version of an application, only to find it's a spoofed alert and they have downloaded a worm or other virus. Another way that users' systems get infected is through *drive-by attacks*, where malware on a website is automatically downloaded to the user's workstation when they visit the site.

Systems administrators would really like to lock down desktop environments, so that users can make only minimal changes to the set-up and any changes they do make are wiped at the end of a session. This *virgin state* ensures administrators can stay on top of software updates more easily and, in theory, eradicates much of the potential for infection.

Locked-down environments are appropriate for public areas or shared-use machines, for job sharing environments (where two or more employees work at the same desk at different times of the day or week), and perhaps even for mobile users. But whether they are right for the wider company is a different question.

Companies should have a staff policy for employees borrowing portable computers — for example, locking down the desktop environment can help enforce this. But you need to consider whether you're hampering employee productivity by doing so.

Ensuring Data Security

Data security measures control access to confidential data and protect it against corruption. It's often in the headlines as politicians and government employees leave their laptops on trains and planes, putting personal information out in the open.

But behind the headlines, businesses have more straightforward concerns over customer details and a legal responsibility to keep their employees' personal data private.

Cybercriminals' ultimate goal is your organization's data.

Realizing the reach of databases

Because of the interconnectedness of systems today, you cannot expect that data on a separate system is secure — the database itself needs securing, as do any applications connected to it, and the operating systems they run on.

Cybercriminals have had a lot of success exploiting databases through web applications that use outdated code and tools. Think about it — if you've got a database connected to a web application, anyone who can gain access through a vulnerability in that application can then set up a query and potentially search through your data for whatever they want.

It's precisely this type of attack that has led to some of the world's largest security breaches, but smaller organizations are just as vulnerable — if not more vulnerable. Data breach notification laws in most U.S. states require organizations to notify affected persons when they occur.

Curbing email threats

Email is a potential minefield for data loss, because it's usually only secured by user name and password. There's some comfort to be taken from the fact that searching for a sensitive email is like looking for a needle in a haystack, such is the volume of messages.

Email is inherently insecure and, for commercially sensitive emails, encryption is still the answer. *Email encryption* uses keys to both authenticate users and protect sensitive information.

There's been much discussion about the perceived privacy of employee email at work. Are emails the personal property of the receiver or the company? But a sensible email policy and disclaimer should protect the company against most email problems. See Chapter 2 for a discussion of acceptable use policies.

Taking care of data

Data loss often occurs when information is passed around a business — on a USB stick, for example, or when someone downloads some data for analysis and leaves it on a laptop.

Data leaks tend to happen when data is in transit — or when employees aren't following the policies the company has established.

Automation can again help in this respect, for example, by automatically encrypting data when it is transferred to a USB stick or employing a solution to ensure data on a laptop is automatically encrypted.

Providing Physical Security

Protecting the business premises, facilities, staff, computer systems, and other assets is probably the most hands-on security job. Although you may think that physical security is out of place in a book on IT security you'd be wrong.

Physical security provides the first line of defense to IT systems and is an essential prerequisite — the easiest way for a cybercriminal to steal data or compromise systems is to gain physical access to them.

Protecting your business premises is probably something you've already planned and provided for and the risks to IT assets will not change your arrangements. However, having conducted an audit of the IT assets in your company, you may

decide some areas are worth extra layers of protection, not just because of the value of the system itself, but because of the data that resides on it, and the disruption that would be caused to the business if it was taken down.

For example, securing access to a server room, if you have one, is essential — and you should screen anybody entering and leaving to make sure they aren't carrying removable media that they could use to steal data.

Locks, safes, alarm systems, and security guards are tried-and-true security methods, and more modern electronic devices can help as well:

- CCTV cameras trained on particular access points with the potential to link to computer networks for recording and viewing anywhere.
- Monitors, cabling, controllers, and so on are increasingly affordable for the small business.
- Alarm systems, not just at the perimeter of the building, but in particularly sensitive positions, are also falling in price and many can now be self-installed.
- Access control systems, with cards, PINs, or entry phones, used to be the reserve of larger companies, but are now essential for all.

Planning for the Aftermath

No security plan is complete without a business continuity and disaster recovery plan. Planning how to stay in business in the face of a disaster, whether technical, as in the website going down, or natural, such as a fire on the premises, is a high priority for any business. *Business continuity* focuses on keeping the business running in the face of such an event, whereas *disaster recovery* is about restoring IT systems after a disaster.

Business continuity planning is often thought of as considering the worst possible scenario and how to recover. Given that you're unlikely to encounter a terrorist attack in your company's lifetime, it's better to think of it as protecting everything from day-to-day scenarios, like power outages and supplier demise or floods and hurricanes.

That said, if you're wondering whether it's really important to have business continuity plans, consider that most small firms that experience a worst-case scenario don't survive:

- Of the 350 firms affected by the 1993 New York World Trade Center bombing attacks, 150 didn't survive. However, those that did, and there are some notable examples, were up and running with minimal disruption a few days after the event.
- The securities trading firm Cantor Fitzgerald occupied several floors of the World Trade Center above the impact zone of the 9/11 terror attacks. The company lost most of their employees, but because they had a disaster recovery plan mostly in place, the company survived.

Hacker attacks and data corruption must, by comparison, seem pretty insignificant. Yet because of their disruption to business continuity they actually rank as one of the more serious threats.

Common business continuity threats include:

- Natural disasters (floods, earthquakes, fires, and so on)
- Cyberattacks
- Internal sabotage
- Utility outages
- Terrorism
- Diseases (such as a flu pandemic)
- Industrial accidents (such as a plane crash, train derailment, hazardous chemical spill)
- IT hardware (for instance, hard drive) failure

After you identify threats, analyze their impacts, and put business continuity plans in place, be sure to test and maintain your systems. Many companies stop after formulating the plan and think they're protected. Not so. It's the testing and maintenance of the plans that proves so critical to their efficacy in the event of a disaster.

Disaster recovery plans, when they are in place, tend to be the most effective in the event actually happening, while plans to address systems failure, website attacks and malware infection are least effective, perhaps because they are less rigorous.

Making Your Users Aware of Your Plans

Communicating the existence of plans, staff policies, and procedures and the do's and don'ts of IT security to your employees is a vital step toward making those plans effective.

Many small businesses don't communicate what they mean by *acceptable use* or what constitutes a strong password. So, while you think best practices are being maintained, your employees don't know what those best practices are. If you don't tell employees what the plans and policies are, how are they supposed to follow them?

Not many people deliberately set out to harm their business or expose it to unnecessary risks, but employees may endanger your business through ignorance of the policies. Seemingly innocuous web surfing or data transfer can lead to alarming lapses that cybercriminals can then exploit, leading to a devastating breach. Whereas you'll appoint individuals to monitor and manage security in the business, protecting business assets is ultimately the responsibility of every employee.

Often the weakest link in an IT security management system is the people. Education and ongoing awareness are the icing on the cake, the all-too-often missing piece of the jigsaw puzzle, the final hurdle in the race for IT security excellence.

Most cybercrime is designed to sucker users into activity that compromises their company. This is activity that — if they thought about it — they would not enter into. It includes:

- Clicking on a link in a spam email
- Visiting a website they really shouldn't be looking at
- Handing over personal or company details to an unidentified third party
- Taking confidential data outside the organization
- Skipping security updates or back-ups to save time

Initial communication of security and staff policies, plus the education about their importance, helps ensure compliance

at least at an outline level. Training should emphasize lowest level of trust — if you're not sure whether an attachment is safe, don't open it.

But ongoing awareness and training is also important to keep ahead of cybercriminals. This is particularly important as threats and policies change and to emphasize to staff the management's ongoing commitment to strong protection. Cybercriminals are always looking at new ways to trick users into doing things they shouldn't, so it is important to ensure everyone is always on their guard. If it looks suspicious, it probably is.

Chapter 4

Knowing Your Enemy

In This Chapter

- Getting an overview of how threats have evolved
- Understanding the main threats your business faces today
- Reading up on some cyberattacks history
- Exploring the cybercriminal underworld

The threat landscape has changed dramatically over the past ten years, from the mass outbreaks grabbing the headlines at the beginning of the decade to today's more covert, combined web threats. There's also been a huge growth in the volume of threats, with antivirus researcher AV-Test now picking up 700,000 new instances of malware a month. The sheer volume makes threats harder to track and more difficult to combat. In addition, the nature of the cybercriminal underground has changed from a bunch of glory-seeking hobbyists to a professional money-motivated industry.

Smaller businesses are more susceptible to targeted attacks, because they often don't have the IT resources to fend off such assaults and can struggle to respond.

In order to be able to defend yourself from the evolving threats, the best strategy is to know your enemy; this chapter examines in more detail modern-day threats and the criminal organizations behind them.

Evolution of the slickest — A short history of cyberthreats

Before and during the early 2000s, mass outbreak viruses, worms, and Trojans were the prevalent form of malware. The Melissa virus, first released in 1999, famously attempted to mass mail itself to the first 50 entries in the user's address book. The ILOVEYOU worm, arriving the following May and reported to be the most financially damaging threat up until that point, again mailed itself to all entries in the user's address book, with a "Love Letter" attachment that caused significant damage on opening. Code Red in 2001 and SQL Slammer and Sasser followed in 2003.

Numerous variants of worm and virus continued to appear and exploit different vulnerabilities, mostly in Microsoft systems (due to their ubiquity), through the following years. Over time, though, the potency of these viruses was limited by organizations doing a better job of locking down their environments, increasing effectiveness of antivirus software, and by users becoming a lot savvier.

Tracking the spam epidemic

Cybercriminals turned to spam mass mailers between 2001 and 2003, using the *phishing techniques* of sending legitimate-looking emails to dupe unsuspecting users into handing over bank account details and other personal information.

The problem of spam reached epidemic proportions by 2004 when 70 to 80 percent of the email entering most businesses could be classified as spam; it was around this time too that virus writers starting attaching their malicious payloads to email messages, creating the perfect storm for IT security professionals.

Again, the tide of spam has been turned somewhat by spam filters that have become more sophisticated, junking not just email that has a suspicious looking message line or sender, but also by content type. Hosted anti-spam technology is tackling the problems further, ensuring that the huge volume of unwanted email is not clogging up mail servers and networks by removing spam and other email-based threats before they get to the network.

Watching spyware

By 2004, *spyware* (unknowingly downloaded software that records the user's computer activity) was added to the cybercriminal's arsenal; a far more sinister and difficult threat to track. According to a 2004 study, by AOL and the National Cyber-Security Alliance, 80 percent of home users' computers had some form of spyware on them, unbeknownst to the user.

The development of spyware was all the more serious because, as it was

emerging, antivirus vendors were still looking the other way. Traditional antivirus products were not designed to detect spyware, which displays completely different characteristics than viruses. Subsequently, spyware has largely been rolled into all-in-one security suites and most businesses will now be covered.

Fighting botnet wars

Next came a further progression from spyware to the *bot*, short for robot. Bots are compromised computers, known as a *botnet* when grouped together, that stand ready to do the bidding of their *botmaster* or *bot herder*, launching attacks ranging from denial of service attacks to mass spam mailers.

Botnets have hundreds to thousands of times the computing power of traditional cyberattacks and can cause serious damage in concentrated, targeted initiatives. Some experts believe modern, distributed computing techniques have aided the spread of botnets, which can quickly infect a wide number of computers through filesharing and peer-to-peer networks.

Guarding Against Today's Combined Web Threats

If the way threats have developed over the last ten years tells us anything (see the nearby sidebar, "Evolution of the slickest — A short history of cyberthreats") it's that as soon as you plug one hole in your defenses you have to guard another. Today, the boundaries between different types of malware have blurred and what was, in the past, a relatively simple, linear attack has turned into a blended, often sustained assault.

Previously, the method of attack came to define it (and often the associated defense), but cybercriminals are becoming more sophisticated all the time. They build on the most potent payloads of the previous generation, while including new methods of attack, and they constantly change their points of attack to avoid detection. Their new attacks combine a number of damaging characteristics to potentially deadly effect.

These blended threats are called *web threats* as they are, for the most part, web-based. A 2008 study from TrendLabs (Trend Micro's security laboratory) tracing the origins of a large

number of computer infections found that over 90 percent arrived at their target via the Internet. Second to the web was file transfer using removable media such as USB drives.

The web provides the perfect place for launching cyberattacks. It provides a mass audience of potential victims, and cybercriminals, to a certain extent, can mask their true identities from the user. Of course, cyberattacks are also easy to trace, as they come from a specific URL or IP address, which can be blocked, but this just forces the criminals to move on to their next prey.

Looking at lethal combinations

Blended web threats are often multi-stage, appearing at first to be benign, for example, an email with a link that when clicked unleashes a malicious payload. Stages might include:

- Malware is installed, through an email attachment or compromised website
- An open communication channel is established (a backdoor), usually through a Trojan horse
- Additional malware is downloaded, possibly changing the form of the original malware

Blended threats harbor several varieties and levels of threat. They are:

- **Multivariant:** Created in large batches of small quantities with endless variations from one batch to another. The variety is an attempt to stay one step ahead of detection.
- **Multiprotocol:** Attacking more than one system. For example, a threat may arrive via an embedded URL in an email, test for vulnerabilities in a browser, or attack via email or IM protocols.
- **Distributed:** Spreading their load over many hosts, again each in small quantities.

Case study of a cyberthreat: The Conficker worm

The Conficker worm or WORM_DOWNAD is a good example of the way cybercriminals combine the traditional mass-outbreak tactics and more modern blended attack mechanisms and "command and control" infrastructure.

The worm exploited a vulnerability in a Windows service to infect Windows PCs and then spread itself around Windows networks; a subsequent variant managed to force its way onto network servers and removable drives, reinfecting previously infected PCs. It's thought to be the widest spreading worm since SQL Slammer in 2003, by January 2009 infecting somewhere between 9 million and 15 million computers.

The worm blocks access to antivirus sites, disables Windows updates, and other Windows services and user accounts are locked out. It generates a list of domain names that it connects to and downloads a further payload.

Microsoft released an emergency patch in October 2008 to repair the vulnerability and formed an emergency group to combat the effects of Conficker that offered a reward of $250,000 for information leading to the arrest of its creators. But many machines remained unpatched.

Much speculation surrounded the eventual payload as the worm's botnet relaunched itself on April Fool's Day 2009, but it has caused little additional damage.

The combination, or blend, of attacks is potentially lethal, using spam for broad-based dissemination, the Internet as the perfect mass medium and malware to perform malicious activity. Any part of the picture may appear benign but, viewed as a whole, the combined assault becomes clear.

Tapping into social engineering

In recent years, criminals have increasingly been using *social engineering techniques* (basically, cyber-lying) to achieve their criminal ends. They piggyback on issues that are in the news or purport to be from your bank or a delivery company in an effort to persuade you to open a malware file or visit a malicious website. They use phishing emails to try to trick personal information out of users, for example, by asking them to fill in a survey that promises some financial reward. Or they

pretend to be social networking sites or even antivirus software providers.

Worst of all, these villains don't just focus on the virtual world. Recent attempts in the physical world seek to drive people to infected websites. One example of this is flyers placed on parked cars stating they have been fined for parking illegally and to go to a website to confirm the vehicle details. Visiting the website then installs malware onto the PC.

An example of a more sophisticated spamming trend is the use of *backscatter spam* in which criminals mass mail a huge number of recipients pretending to be a different sender. The third party then receives a whole load of failure or out-of-office messages.

Raising the volume

The growth in the volume of malware generated today is phenomenal. According to AV-Test, in 1988 there were 1,738 unique threat samples. By 2005 more than double that number were being added *every year*. But over the last few years the number of new threats has exploded. Here are some statistics to blow your mind:

- In early 2008 the total number of unique threats in existence exceeded 10 million; by the end of 2008 it had reached 20 million — effectively doubling in less than a year!
- On average, over 2,000 new, unique malware threats hit the Internet every hour.
- It now takes less than a week to produce the entire malware output of 2005.

According to TrendLabs, 3.5 new threats are released every second by cybercriminals. Many of those threats involve spam and bots, which are intrinsically linked, because botnets are some of the main spam generators. In a recent laboratory-controlled investigation, a single bot-infested computer generated 2.5 million spam messages in a 24-hour period.

Entering the Cybercriminal Underworld

Unlike the real-world economy, the cybercrime economy is booming. According to some estimates, the cybercriminal underworld is now worth as much as $100 billion a year in profits. As the stakes get higher, the underground is becoming more professional and is increasingly structured as a business. This means people are specializing in offering particular disruptive services and almost anything is available to buy or rent.

As well as packaged options, cybercriminals can employ the services of dedicated malware programmers, selling code online just like a legitimate software development firm.

Counting the money

Stolen information is big business, with cybercriminals dealing in personal information, including email logins, credit card numbers, social security numbers, account passwords, PIN numbers, and gaming passwords. Cybercriminals do business with botnet vendors and hackers, dealing in the produce of malware vendors, who in turn are collaborating with anti-detection vendors and toolkit vendors. Carders, spammers, and blackmailers work alongside or sometimes collaborate with these independent businessmen in what is becoming an increasingly joined-up industry.

Prices on the black cybermarket, meanwhile, are surprisingly affordable, with $50 to $3,500 buying you off-the-shelf malware, according to an article in the *Independent*, and a subscription to a service that monitors antivirus developments and tweaks malware accordingly costing $25 to $60 per month. According to the article, an hour of usage of a botnet network of 8,000 to10,000 computers costs approximately $200. Research from TrendLabs on the underground digital economy in 2007, meanwhile, found that for just $100 a day you can have a distributed denial of service attack

while $1,000 will purchase 10,000 compromised PCs. Denial of service attacks are designed to take online resources out of operation by bombarding them with service requests.

Employing a host of tools

One of the reasons for the increasing success of cybercriminals is the availability of tools that get them up and running fast. These range from free, off-the-shelf phishing kits from the likes of Mr. Brain, a group of Moroccan fraudsters advertising easy-to-use kits that have launched attacks on many tier-one banks, to free spam templates that exactly replicate the appearance of popular banking websites.

Data breaches are on the rise: according to the Identity Theft Resource Center's 2009 breach report, 498 breaches were reported at the end of 2009, an increase over 2007's total of 446 and representing a total of 222 million data records compromised.

Equally worrisome is the growth of automated malware generation programs that can take one instance of malware and generate hundreds of variants each with a unique footprint, thus evading the traditional pattern-file detection.

Chapter 5

Devising Practical Solutions

In This Chapter

- Feeling swamped by the rising tide of threats
- Facing threats from every direction
- Heading to the cloud for protection
- Linking to the Smart Protection Network

With the number of IT threats increasing exponentially year after year, security vendors sometimes seem like they're trying to hold back the waves. Although companies are generally getting the message about IT security and are implementing the measures we talk about in Chapter 3, traditional means of protection will not be adequate in the future.

Pattern file updates, explained later, are not only getting larger and more frequent — they are also becoming less effective, as cybercriminals are constantly changing their attacks and using combined web threats to hide their intentions.

Consider cloud computing as the savior of IT security; it's been adopted elsewhere for solutions that need to keep large data stores offsite and constantly updated. And it significantly eases the administrative overhead for the small business.

The Trend Micro Smart Protection Network goes one step further, taking the idea of cloud computing and linking everyone's clouds together. It's the type of shared resource that modern computing demands — a neighborhood watch scheme for IT security.

Trying Vainly to Hold Back the Tide

The rising volume of malware over the past few years has been phenomenal. But it's only going to get worse in the coming years. TrendLabs noted a 1,731 percent increase in incoming threats between 2005 and 2008 and by 2015 it predicts will be processing 26,598 threats per hour, as shown in Figure 5-1.

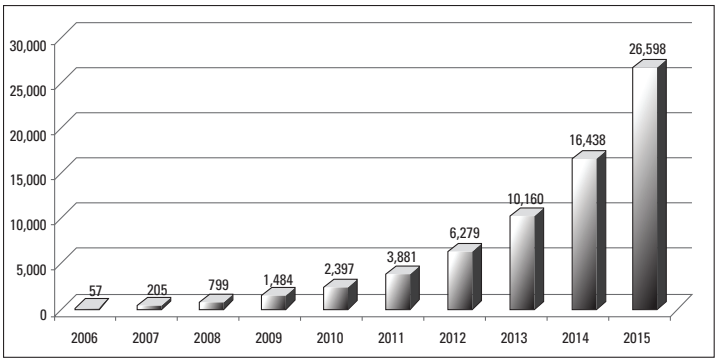

Figure 5-1: The projected increase of incoming malware threats.

Part of the reason analysts can so confidently predict that the rising tide of malware will continue to swell is the vicious circle that now engulfs computer networks. For example, in the United States, despite significant activity and regulatory measures to combat spam, it continues to grow as new spam and phishing initiatives emerge. The United States is still way ahead of any other country, accounting for 22.5 percent of all spam. And the inevitable increase in the number of bots will lead to more spam, denial of service, and other IT attacks.

The McColo effect

If you need further evidence of the continuing prevalence of threats, 2009's McColo affair provides it. McColo Corp was a San Jose-based Internet hosting provider that was believed to house all sorts of cybercriminal operators, from spammers to the command-and-control infrastructure for some of the world's largest identified botnets. These botnets controlled thousands of PCs involved in spam, malware, child porn, credit card theft, fraud, and get-rich-quick scams.

After years of investigation, McColo was finally shut down in November 2008, leading to an immediate drop in the world's junk email of 50 to 75 percent. However, the effect of disconnecting McColo was only temporary; spam levels gradually started creeping back up, and one of the largest botnets that was thought to be housed at McColo appears to be gaining in strength, controlled from elsewhere.

Signature files can't keep up

The proliferation of threats makes it difficult for traditional safeguards, such as pattern file or signature updates, to keep up. Most modern, antivirus systems look for virus patterns by scanning computers for a particular signature and matching it to a database of pattern files it holds. When a match for a signature is discovered, the offending item can be quarantined or deleted altogether.

Back in 1988, when there were 1,738 unique threat samples, security professionals grouped these into just 30 families or patterns and needed to issue 30 signatures that their scans could match malware to. Entirely new patterns would only emerge slowly as virus writers found a new method for spreading their payloads.

Now thousands of new patterns emerge every hour, and cybercriminals, realizing the limitation for vendors of having to issue updates, are constantly creating new variants of their malware. Often, they change malware within hours of issuing it to stay ahead.

The security industry has reacted to this problem by issuing more frequent updates with some vendors refreshing security measures twice a day or even hourly. Each new update contains a higher volume of patterns as security vendors try to hold back the tide of cyberthreats.

But frequent pattern file updates come at a cost. They can:

- Choke network bandwidth as they update client machines
- Cause a drag on the performance of individual PCs
- Provide an extra headache for network administrators as they check machines are being kept up to date

The rate and volume of pattern updates is clogging up corporate networks, choking precious bandwidth that should be used for important business tasks, and affecting the performance of user machines. There's nothing more irritating than having to wait for your machine to finish an update when you boot it up in the morning and just want to be able to start working right away.

Meeting the New Challenge of Blended Threats

Some indications seem to suggest that companies' security measures and their protection against business-disrupting threats is getting better. The Verizon/Secret Service and Identity Theft Resource Center surveys show that the number of breaches reported in 2009 was less than in 2008 (657 versus 498). Although it's hard to know whether the actual number of breaches is increasing or decreasing, we do know that IT security is getting more attention every year, and the tools for protecting IT systems are more plentiful and easier to use.

Adding on multiple threats

Traditional IT security measures deal with traditional security challenges, but what about the newer threats that avoid these technical controls, such as *data-stealing malware*, which infects corporate networks and sits undetected, silently stealing

corporate information for fraud. Data-stealing malware is one type of combined web threat, usually made up of a number of threats, merging seemingly innocuous activity with a malicious payload, as shown in Figure 5-2.

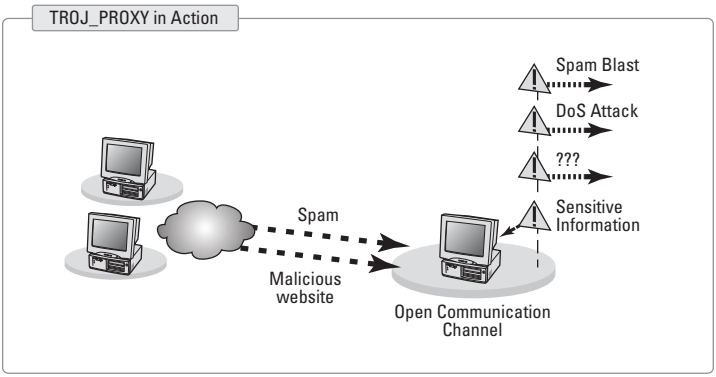

Figure 5-2: A combined web threat from spam and malicious websites.

Blended web threats are able to change form from what seems an innocuous program into something malicious, thus evading file-based scanning. They often arrive via the open web protocol port, thus evading intrusion detection systems like firewalls, or via an embedded link within an email.

The email filter will scan any attachments in an email, but if a user can be persuaded to click a link in the email it takes them off to a bogus site run by the cybercriminal, which then starts downloading malware.

Increasingly, too, cybercriminals are expanding their range of targets to include mobile phones — specifically the iPhone IOS, Windows Mobile 7, Android, Blackberry, and Symbian. The increasing corporate use of these devices is creating a whole new headache for systems managers who felt like they were just getting user workstation management under control.

Cybercriminals constantly test their new malware against file-based scanning products, and so effective are their attacks that many enterprise security products are just not able to detect them. Because the threats are constantly morphing and changing the pattern of attack, signature-based or behavior-based file scanning is ineffective.

Facing danger from the web

Business websites are increasingly being compromised by cybercriminals with automated tools that crawl the Internet looking for vulnerabilities.

Of course, big sites like eBay and Google are prime targets, but cybercriminals also get a lot of mileage out of small business websites. These are often older sites using tools and software that have not been updated — again because a firm doesn't have dedicated resources to keep it up to date.

Websites are increasingly being compromised. WhiteHat Security's latest figures show 64 percent of sites with a high or critical vulnerability, while, according to Websense, 70 percent of the top 100 websites contain malicious content or a hidden redirect.

Keeping on top of compromised sites across different geographies when they are infected at such alarming rates is one of the toughest challenges facing the security industry today.

Finding Security in the Cloud

Cloud computing is a pool of shared IT resources, usually maintained off the company's site, although in large companies it can remain in-house in a private cloud. Cloud-based services include hosted email security and hosted web and file reputation databases — the stores that hold details of risky websites and file names. Turn to Chapter 2 for more on hosting services. Moving pattern file databases and other security resources into the cloud is one solution to the problem of the rising tide of threats.

The advantage of using cloud computing to manage large pools of resources is that the cloud is maintained by experts, so you don't have the hassle of looking after it in-house. It's also:

- Scalable, so it can comfortably get bigger as you have more resources to host.
- Virtualized, which is another way of saying it makes the best use of the IT resources it runs on, and, related to that, it's less resource hungry.

- More reliable as you're not relying on your own network keeping current. As long as you have an Internet connection, your machines can update themselves.
- Cheaper than keeping the resources locally, although the cost depends on the number of users and size of the database you're using.
- Effective across multiple endpoints, so you can easily connect mobile workers, different mobile devices, and so on without having to physically go around and update them. It makes security no longer dependent on location.
- More secure. There's been much discussion about the security of cloud computing platforms. But think about it: You've got the security vendor hosting its own software, rather than you trying to run it off your own systems. It may have gone out of your control, but it's bound to be safer.

The added benefit of running security in the cloud is that you can combine different cloud services and have them talk to each other. This combats the extra threat provided by combined web threats, by spotting the patterns in the combinations themselves.

Exploring the Smart Protection Network

The Smart Protection Network is a new approach that takes advantage of the latest technologies.

With security resources already being stretched to the limit, and the situation continuing to get more challenging, the Smart Protection Network's dynamic real-time protection technology is designed to scale with the nature of the threat and have less impact on the network and PC resources than traditional offerings.

The cloud computing-based Smart Protection Network consists of three elements:

- Email reputation management (estimating the authenticity of email addresses based on similar addresses held on file)
- Web reputation management (or web threat protection)
- File reputation management (or Smart Scan)

It gives you:

- Cross-correlation between events, so if a spam links back to a particular website, that URL can be added to the blacklist, and the malware behind that website can be analyzed and a signature written to identify and stop it
- Cross population between databases on a global basis, updating security breach information from, say, the Asian market to the North American market
- A feedback loop from individual users, all effectively sharing information about threats they encounter

The security vendor maintains the global network of threat intelligence data, adding millions of suspect IP addresses, URLs, and files a day. And, because it's hosted, the network can process billions of requests a day, providing comprehensive protection against all types of threats, including new-style web threats.

Correlation is an important concept when combating blended threats. It's the combination of the three elements defined previously that makes the Smart Protection Network so powerful in combatting web threats. The network is able to link between different events, helping build up a global picture and ultimately making for a better threat database.

The Smart Protection Network uses global feedback loops to track back from a security threat and isolate its cause, linking together research centers, users, products, and services:

- When malware is detected, the network generates feedback that leads to the investigation of the originating URL and updates the Smart Protection Network accordingly.
- The email is, in the future, blocked at the network gateway, because it contains a URL that is now blacklisted in the Web reputation database.

- Further downloads are blocked, because the file pattern is added to the file reputation database and the email sender is added to the email reputation database, breaking the chain of infection at the earliest opportunity.

Using a cloud gets faster results, too, because you're not waiting for machines to download the latest pattern file updates.

The Smart Protection Network is sometimes compared to an online version of the Neighborhood Watch scheme, where citizens look out for each other in real-time and head off trouble before it occurs.

Looking into the Future of Security

With security resources already being stretched to the limit, and the situation continuing to get more challenging, the combination of cloud-based technology with traditional protection methods points the way to the future of security and, in tests, it gives the best levels of protection.

For example, in a January 2009 anti-spam comparison report by West Coast Labs the hosted email security option had the highest detection rate (at 96.71 percent) when compared with nine other solutions, as well as a negligible false positive rate.

Another example was in November 2009 when NSS Labs tested the latest security solutions. The test showed how important the combination of cloud and client (locally hosted) protection is, with the winner giving 96.4 percent protection against modern real-world threats.

In October of 2010, NSS Labs reported that consumer antivirus programs were falling behind. This news underscores the need for businesses to use anti-malware software designed specifically for business.

In a not-too-distant future, different technologies and approaches will come together to show the way forward for IT protection. For small businesses, this not only keeps assets more secure, it also makes managing security easier and less expensive.

Chapter 6

Top Ten IT Security Measures for Small Business

In This Chapter

- Knowing what you're up against
- Finding ways to fight it

This short chapter offers the essential practices that every small business needs to adopt to keep IT security systems working effectively. We trust your business scores ten out of ten!

Identify Threats

Every business with an Internet connection — in fact, every *person* with an Internet connection — is prey to some types of cybercrime. To fully protect your technology and your business, you need to evaluate which threats are of most concern. Chapter 1 helps you evaluate your at-risk areas to identify events that could affect your business and its continued well-being.

Conduct an Impact Analysis

After you identify threats to your business you need to determine the potential harm if they're realized. Run through all the what-if scenarios you can think of so that you can start

picturing how to recover if those what-ifs came true. Turn to Chapter 1 for tips on how to conduct an analysis.

Write a Security Policy

The measures you put in place to make your business secure form the security policy that guides business practices and employee behavior. Chapter 2 covers this topic in depth.

Identify Assets and Risk Factors

You need to know what valuables you have in order to come up with a way to protect them. And looking at the risks that threaten each asset helps you devise protective measures.

Write an Acceptable Use Policy

Your business supplies the tools your employees need to do their jobs. Your employees need to know what is and is not acceptable use for each of these tools. For example, you need to prohibit your employees from visiting websites that could get both them and you in trouble with the law. But, as Chapter 2 explains, it's not just illegal use you want to curb, but all use that affects productivity and good business practices.

Write an Internet and Email Policy

Two of the main tools you provide for your employees are access to email and the Internet. Have a policy in place to guide employees in the proper, businesslike use of these tools. Chapter 2 offers suggestions.

Establish Technical Controls

Every business needs to have certain systems in place to protect IT functions. Make sure that you cover the basics by constructing firewalls and purchasing antivirus/anti-spyware software. We talk about defensive measures in Chapter 3.

Coordinate Security Elements

You have a range of security measures to protect a range of vulnerabilities. All these security controls need to fit together, so that all your security controls and employee practices and policies form a united front to guard your business. Chapter 3 has more info on how to make things work together.

Know Your Enemy

You need to know how cybercriminals operate. And you need to stay on top of emerging threats, such as blended web threats, so that you can educate your employees to meet these threats. Chapter 4 covers the latest tricks and threats.

Harness the Power of Cloud Computing

Cloud computing, which enables you to use resources from a secure, shared data center, gives you better levels of protection and reduces the impact on your network and computing resources. We go into the cloud in Chapter 5.

Stay secure from IT threats

IT security threats are everywhere and new ones seem to emerge every day. But if you're a small business, you have limited resources to protect your valuable assets. This book gives you the basics you really need to be secure. Outlining the major threats and how they could affect your business, it helps you craft a security policy, put together a coordinated defense, and, most importantly, manage security better. Cybercriminals are constantly moving in with new methods of attack — here's how to stem the rising tide.

- ***Understand security threats* — they're everywhere; you need to be able to identify and understand them**
- ***Develop a comprehensive security policy* — even if you don't know what to expect, you can figure out how to handle the unexpected ahead of time**
- ***Defend yourself* — you need a coordinated defense that will repel intruders at all levels**
- ***Know the enemy* — understand who's creating the different types of threats and the best ways to defend against them**
- ***Figure out solutions* — to help fight against threats, you need to know who can help**

Open the book and find:

- **A list of security measures small businesses can take**
- **How to gauge the impact of threats on your business**
- **Information on educating employees**
- **A sample acceptable use policy**
- **An overview of how threats evolve**

Making Everything Easier!™

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

For Dummies®
A Branded Imprint of
WILEY

ISBN: 978-1-118-08410-6
Not for resale