Making Everything Easier!™

Symantec and DLT Solutions Special Edition

Cybersecurity FOR DUMMIES®

Learn:

- **Why you need a cybersecurity solution**
- **How to protect your information**
- **What goes into cybersecurity**

Brought to you by

Symantec. DLT SOLUTIONS

Brian Underdahl

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help our customers, from consumers and small businesses to the largest global organizations, secure and manage their information-driven world against more risks at more points, more completely and efficiently. As the world's fourth largest independent software company, our unique focus is to eliminate risks to information, technology, and processes independent of device, platform, interaction, or location. Our software and services protect completely, in ways that can be managed easily and with controls that can be enforced automatically, enabling confidence wherever information is used or stored.

About DLT Solutions

Through the partnership with Symantec, DLT Solutions provides data protection, management, availability, and disaster recovery software solutions to government agencies and businesses. Symantec delivers information security and availability solutions that provide customers with a more effective way to secure and manage their most valuable asset: information.

With its product portfolio, multiple procurement vehicles, and award-winning track record, DLT Solutions confidently supports public sector clients in the technology implementation required to achieve their agency missions. DLT was recently honored as number one in the Term Software License category in the GSA IT Catalog of Top IT Contractors on GSA Schedule 70. For more information or to place an order, contact DLT Solutions at 888-358-4472, email sales@dlt.com, or visit www.dlt.com.

Cybersecurity FOR DUMMIES®

SYMANTEC AND DLT SOLUTIONS SPECIAL EDITION

by Brian Underdahl

Wiley Publishing, Inc.

Cybersecurity For Dummies®, Symantec and DLT Solutions Special Edition
Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-118-01137-9

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Jennifer Bingham

Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Lavonne Roberts

Proofreader: Dwight Ramsey

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Diane Graves Steele, Vice President and Publisher, Consumer Dummies

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

Table of Contents

Introduction

There's no denying that cyberthreats are a big concern to anyone who has responsibility for the computing resources of an organization. Viruses, worms, spyware, and many other types of malware are all waiting for the slightest opportunity to invade and attack. Cybersecurity is your defense against the criminals who want to compromise your organization's computer systems.

About This Book

Cybersecurity For Dummies, Symantec and DLT Solutions Special Edition, shows you the threats that make securing your systems so important. You'll see some of the trends that show where cyberthreats are headed and the multiple layers that must be protected.

As a government organization, you need to be aware of the guidelines and mandates that dictate what you must do to protect your systems and the sensitive information they contain, so I give you an overview of these important items. Finally, I introduce you to some of the Symantec products designed to help keep your systems safe.

How This Book Is Organized

This book is divided into five chapters. Here's a brief breakdown of what you'll find in each of the chapters:

- **Chapter 1, Cybersecurity 101.** Chapter 1 tells you the basics of cybersecurity and gives some insight into why the cybercriminals are so intent on invading your systems.
- **Chapter 2, Understanding the Layers of Cybersecurity.** Chapter 2 shows you the different layers of your computing environment that need their own targeted types of protection.

- **Chapter 3, Looking at the Federal Cybersecurity Guidelines.** In Chapter 3 you see the important federal standards that you must follow to keep your cybersecurity efforts in compliance.
- **Chapter 4, Examining Symantec's Cybersecurity Ecosystem.** Chapter 4 shows you a number of Symantec products that can make your life easier by providing the cybersecurity solutions you need.
- **Chapter 5, Top Ten Cybersecurity Suggestions.** In Chapter 5 you find ten very useful reminders of good practices that will greatly reduce your risk level.

Icons Used in This Book

This book uses the following icons to call your attention to information you might find helpful in particular ways.

The information in paragraphs marked by the Remember icon is important. You can easily spot the information when you refer to the book later.

The Tip icon indicates extra-helpful information.

This icon marks places where technical matters, such as pixels and whatnot, are discussed. Sorry, it can't be helped, plus the information is intended to be helpful.

Paragraphs marked with the Warning icon call attention to common pitfalls that you may encounter.

Chapter 1

Cybersecurity 101

In This Chapter

- Understanding cybersecurity
- Getting to know the threats
- Realizing the economics

The Internet continues to grow and become more a part of daily life with each passing day, so it's no surprise that the dangers and threats associated with the Internet are growing, too. The bad guys are out there and they're just waiting for a chance to make your life miserable.

As a government agency you're trying to provide needed public services in the most efficient way possible. But in order to provide those services you have to make sure you understand the threats, so this chapter will help you do just that — understand who and what is out to get you!

Understanding Cybersecurity

Wouldn't it be nice if you didn't need to worry about security? Unfortunately in the real world we do have to worry about security — especially *cybersecurity*. But just what is cybersecurity, anyway?

Cybersecurity isn't a single, easy-to-categorize item but a term that covers a number of different areas. Still, if you really get down to the nuts and bolts, you could say that cybersecurity is about protecting information that is stored on computers. Sounds simple, but when you look at how many ways that information is threatened, you begin to realize that cybersecurity really means a whole bunch of techniques wrapped into a single word.

The first computer viruses

The first computer virus was detected on ARPANET (Advanced Research Projects Agency Network — the forerunner of the Internet) in the early 1970s. Called Creeper, the virus gained access via the ARPANET and copied itself to the remote system where the message, "I'm the creeper, catch me if you can!" was displayed. The first known virus meant to attack personal computers appeared in 1981. It was the "Elk Cloner" virus, and it attached itself to the Apple DOS 3.3 operating system and spread via floppy disk.

The Internet continues to expand and enable new ways of doing business and communicating. Social networking, cloud computing, and virtualization continue to gain traction and are rapidly becoming integral to how business and leisure pursuits are conducted online. These technological advances also bring additional challenges for the security industry such as the continued growth of persistent threats, the continued evolution of social networking sites as the means of attack and infection, the difficulty of effectively securing emerging technologies, increases in the sophistication of social engineering, and the continued expansion of the underground economy. Cybersecurity must address each of these threats as well as any new ones that have yet to appear — viruses are only one of the many threats that need to be considered.

The rise of the Internet and increasingly connected computers have certainly been a major contributor to the need for cybersecurity. Before computers were interconnected it was relatively easy to protect individual computers — you just locked the door and the bad guys couldn't get in. Of course the fact that the computers were totally isolated also made it difficult to share information between systems. Because information sharing is at the heart of how useful and important computers have become to today's society, cybersecurity techniques have been developed that balance the need to protect and the need to share.

Understanding Why Cybersecurity Is Important

Government and critical infrastructure organizations are the targets of a wide variety of attacks. For example, the exposure

of critical information through cyberattacks can be very costly to government institutions and may even pose a threat to national security. Cybersecurity techniques provide the critical defenses needed to protect against these attacks.

Government-run Web servers provide a variety of services for government and critical infrastructure sectors, such as hosting publicly available information, customer support portals, and online stores. Some Web servers also enable employees to perform routine job-related tasks from remote locations. A Web server may be a portal to an organization's internal network and database systems. The wide range of uses of Web servers provides an enticing target for attackers.

Attackers who compromise Web servers may be able to access critical information that could expose customer and employee identities and financial details that may be sold in the underground economy. Attackers can also use the server to host malicious code and launch attacks against legitimate visitors of the Web site. Compromised Web servers may also have their publicly accessible content defaced to contain lewd material or misleading and false information.

It can cost a lot of time and money to try to locate and prosecute the perpetrators or to handle lawsuits initiated by people whose information was exposed. In addition, attacks that disrupt customer or employee access to services can result in losses to revenue or productivity loss from employees being unable to perform their job-related duties. Obviously it's far better to prevent the attacks in the first place than to try to clean up the mess after an attack has happened.

The following sections take a closer look at some trends that show where cybersecurity is headed.

Seeing the growing threats

If you want to defend yourself, it helps to know what threats there are waiting for you. Symantec monitors the cybersecurity universe and has gathered some very interesting data that shows what is happening. Here is some of that information:

- In 2009, the United States had the most overall malicious activity measured by Symantec, with 19 percent of the total.
- The United States was the top country of origin for Web-based attacks in 2009, accounting for 34 percent of the worldwide total.
- The top country of origin for attacks targeting the government sector in 2009 was China, which accounted for 14 percent of the total.
- The top Web-based attack in 2009 was associated with malicious PDF activity, which accounted for 49 percent of the total.
- The most common type of attack targeting government and critical infrastructure organizations in 2009 was Web server attacks, accounting for 46 percent of the top 10 attacks.
- In 2009 physical theft or loss accounted for 37 percent of data breaches that could lead to identity theft.
- The United States was the country most frequently targeted by denial-of-service attacks in 2009, accounting for 56 percent of the worldwide total.

As this data shows, the United States is right in the thick of it when it comes to cyberthreats and malicious activity.

The dark side of social networking

People like to socialize, so it shouldn't come as a surprise that *social networking* sites like Facebook, LinkedIn, and so on are popular. It's probably no surprise that the popularity of these sites extends to government workers as much as it does to the private sector, either.

Social networking sites should be of particular concern to government organizations. Not only does social networking provide many potential threats, but social networking sites can create security issues for the organization and its employees. These issues include the potential loss of confidential information, bandwidth issues to support operations, and the possible exposure of the organization to liabilities from compliance concerns. One recent example of the problems made possible by social networking sites occurred in July 2009, when the new head of the British foreign intelligence service

was identified publicly by his wife's posts on her profile on a social networking site. Talk about blowing your cover!

Some problems can be compounded by government organizations having differing responses to social networking. For example, the U.S. Army has issued guidance to its soldiers as well as to civilian employees regarding social networking and what should and should not be disclosed, while the U.S. Marine Corps has banned all access to social networking sites from its network.

To effectively manage social networking within government networks, clear policies on access to these sites is required, along with appropriate countermeasures to prevent unauthorized information from being posted. Because these sites are also often accessible from the outside, you need clear guidelines about what should or should not be posted (such as security clearance data and deployment dates and positions) to these sites.

Phishing your way to success

Phishing is an attempt to obtain confidential information from an individual, group, or organization by mimicking a specific brand for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

One development that Symantec has observed from the increased sophistication of targeting phishing attacks is an increase in *spear phishing* campaigns. Spear phishing is a targeted form of phishing in which the apparent source of the e-mail is likely to be an individual within the recipients' organization and generally someone in a position of authority. These attacks are likely to target senior officials of organizations who have access to significant amounts of their organizations' intellectual property, because successful attacks are likely to garner greater financial yield for attackers.

Understanding the trends

If cyberthreats were always the same, it would certainly be much easier to defend against them. But as Symantec's

research has shown, the threats continue to change and this means that you need to be agile and ready to do battle on new fronts. To help put the ever-changing nature of cyberthreats in perspective, take a look at some highlights of the trends Symantec has discovered:

- Symantec created 2,895,802 new malicious code signatures in 2009, a 71 percent increase over 2008; the 2009 figure represents 51 percent of all malicious code signatures ever created by Symantec.
- *Trojans* made up 51 percent of the volume of the top 50 malicious code samples reported in 2009. Trojans are a piece of malicious code that seems like an indispensable program such as a codec required to view a video or a fake antivirus program.
- The percentage of threats to confidential information that incorporate remote access capabilities increased to 98 percent in 2009.
- In 2009, 89 percent of threats to confidential information exported user data and 86 percent had a keystroke-logging component.
- In 2009, propagation through file-sharing executables accounted for 72 percent of malicious code that propagates.

What these figures show is that the threats aren't only increasing, but they're becoming more sophisticated in their ability to steal sensitive information. In the next section, I examine the reasons why stealing information has become such a high priority.

Commercialization of Threats and Exploits

The famous bank robber Willie Sutton has been quoted as saying that he robbed banks because that's where the money was. The people who create cyberthreats follow the same line — they steal information from computers because that's how they make their money. There is a whole *underground economy* dedicated to commercializing the cyberthreats and exploits discussed throughout this chapter.

The underground economy is an evolving and self-sustaining black market where underground economy servers, or black market forums, are used for the promotion and trade of stolen information and services. This information can include Social Security numbers, credit card numbers, debit card information, user accounts, e-mail address lists, and bank accounts. Services include cashiers, scam page hosting, and job advertisements such as for scam developers or phishing partners.

Stolen credit card info

In 2009, credit card information was the item most frequently advertised for sale on underground economy servers. Credit card information advertised on the underground economy consists of the credit card number and expiry date, and may include the name on the card (or business name for corporate cards), billing address, phone number, CVV2 number, and PIN.

The prices of credit card information advertised in 2009 ranged from $0.85 to $30 per card number. There were three main factors that influenced the prices: the amount of information included with the card, rarity of the card type, and bulk purchase sizes. Credit cards that bundled in personal information such as government-issued identification numbers, addresses, phone numbers, and e-mail addresses were offered at higher prices. Cards that included security features such as CVV2 numbers, PINs, and online verification service passwords were also offered at higher prices.

Credit card information can be obtained through a variety of means, such as monitoring merchant card authorizations or breaking into databases. Data breaches can be very lucrative in the underground economy. For example, a security breach of a credit card payment processor in January 2009 resulted in the exposure of more than 130 million credit card numbers. Even using the lowest advertised price-per-card number in 2009, this breach represents over $110 million in potential profit.

Bank accounts

Bank account credentials were the second most commonly advertised item on underground economy servers, accounting

for 19 percent of all advertised goods. Bank account credentials may consist of account numbers, bank transit numbers, account holder names and/or company names, and may include online banking passwords. Advertisements often include the account type and balance as well as name and location of the financial institution. The advertised prices for bank account credentials depend on the account type, location, and the funds advertised as available. In 2009, prices for these credentials observed on underground economy servers ranged from $15 to $850.

The ability to directly withdraw currency from a bank account is advantageous and attractive to criminals, who can realize a more immediate payout than with online purchases, which need to be sold to realize a purely financial reward. Bank account credentials also allow access to full balances in the bank accounts, whereas credit cards may have daily or other transaction limitations on accessing the maximum available credit.

E-mail accounts

The third most common item advertised for sale on underground economy servers was e-mail accounts. The advertised prices of e-mail accounts in 2009 ranged between $1 and $20 for each account.

Compromised e-mail accounts can also often provide access to additional sensitive personal information such as bank account data, student identification numbers, mailing addresses and phone numbers, or access to other online accounts (social networking pages, online stock accounts, and so on) that people often store in saved personal e-mails.

Chapter 2

Understanding the Layers of Cybersecurity

In This Chapter

- Protecting the multiple layers
- Reporting security incidents

To provide true protection, cybersecurity solutions must provide defenses wherever they're needed. Layered defenses make sense because there are so many different ways that your computers can be attacked. If there were only one type of threat, you would need only one type of security.

In this chapter, I discuss the many different layers that must be protected in order to ensure the safety and integrity of your systems.

Protecting the Multiple Layers

At first glance, it might seem like it would be possible to provide the necessary cybersecurity protection using a single solution. After all, why can't you just put up a barrier that will stop any type of threat?

To understand why a single solution to cyberthreats isn't really the answer, it might be helpful to think of your computer systems as being like a house with its many different components. A few of the protective systems you might find in this hypothetical house could be:

- A roof to prevent rain from pouring in and soaking everything.
- Windows to keep out rain, cold, heat, insects, birds, and such.
- Doors to allow residents to enter and exit, but which could be locked to keep out unwanted visitors.
- Window curtains or blinds to provide privacy.

Although each of these systems provides protection against certain types of threats, none of the systems can do the whole job alone. Taken together, though, they all work in concert to provide a safe, comfortable environment where the entire family can live.

Just as the different components of our house work together to provide more complete protection, different cybersecurity components are needed to protect your organization's computer systems and the information contained on or processed by those systems.

The following sections take a closer look at some of the important layers that need specialized protection to keep your computer systems safe and secure.

Protecting the network layer

When was the last time you saw or used a standalone computer that had no connections to other computers? It's probably been years. Oh, sure, you might occasionally use a computer that temporarily isn't connected — such as a laptop during your morning commute on the train — but you'll probably connect to the network as soon as possible so that you can communicate, exchange files, and so on.

People nowadays live in a connected world, and it's the various networks that make these connections possible. Whether you're talking a small intranet that connects a few computers in a single office or the Internet that connects millions of computers around the world, networks make our computers far more useful than they could ever be without the resulting communications capabilities.

Unfortunately, it's not just memos, reports, and e-mail that can travel across our networks. The same communications ability that makes networks so useful also makes networks a prime path for many cyberthreats, too. As a result, one of the first layers you need to protect is the network layer — the computer communications pipeline that serves your organization.

To begin protecting your network layer, you can start with technology called *network intrusion protection*. This can be deployed directly onto your network or as a software package on your computer. Similar to the way a personal firewall works, this countermeasure watches network-layer communications and processes and protects them against threats such as network-based worms.

Basic implementations of network intrusion protection are *signature-based* and are, therefore, only effective against known attacks. Signature-based means that the system contains a database of known threats — each identified by a known pattern (or signature) — and when a threat's signature is recognized, the countermeasures are activated against the threat. Typically this means that the malicious network traffic is blocked and an alert is generated to a network or security response team to investigate further.

Providing protection against unknown network-layer attacks depends on incorporating further, advanced mechanisms. Chief among these is the use of vulnerability-based signatures. Rather than using a database of known threat signatures, using vulnerability-based signatures involves predicting the characteristics of threats on the basis of the characteristics of the vulnerability they will be seeking to exploit. In other words, once a new vulnerability is disclosed, researchers develop and encourage deployment of signatures that anticipate the nature of yet-to-be-created threats. Essentially, this type of protection depends on recognizing a type of action rather than looking for a known threat — sort of like being on the lookout for activity that indicates the bank is being robbed rather than trying to catch a known bank robber in the act.

In a sense, detecting an attempted network intrusion and preventing an actual network intrusion are two different things. In the bank robbery example you might think of the security cameras as the intrusion detection system and the armed guards as the intrusion prevention system.

Securing the storage layer

Okay, it's time for a snap quiz. Can you name the most valuable piece of your entire computer system? I'll give you some hints — it's not a big fancy speed-demon workstation, it's not your brand-new server loaded to the gills with memory and hard disks, and it's not that huge monitor sitting on someone's desk. Give up? Well the answer is really pretty simple if you think about it. The most valuable part of any computer system is the data that's stored on the system. Anything else is just hardware or software that can easily be replaced.

Stored data is extremely valuable. The criminals who inhabit the underground economy are willing to pay millions of dollars for stolen data such as credit card numbers, bank account info, and sensitive national secrets. (This is discussed in more detail in Chapter 1.) That's why it's so important to secure the storage layer of your systems.

What, exactly, is this storage layer? In most organizations the storage layer primarily consists of file servers or *Network Attached Storage* — NAS — units. In either case, the network administrator can control access to files and folders on an as-needed basis. Some of the tools available to control and protect storage layer access include:

- Usernames and passwords to grant or deny access.
- Encryption to ensure that stolen data will be inaccessible.
- Granular controls that, for example, allow certain users to read but not modify data.
- Data Loss Prevention solutions can ensure sensitive data isn't on file servers and databases.

Depending on the types of data and services your organization uses and provides, you may have additional regulatory requirements to monitor and report on data access in addition to simply controlling that access.

Safeguarding the endpoint layer

The most visible layer of any computing environment is typically the endpoint layer. This layer consists of the devices that end-users use to access their environments. Usually you

may think of these devices as being the PCs, terminals, or workstations scattered around in the office, but they can also be mobile laptops, smartphones, or even the home PCs used by employees to remotely access the services provided by your organization.

Underestimating the scope of endpoint security responsibilities is a common issue that leads to diminished effectiveness, as well as the creation of a patchwork of multiple, potentially independent, solutions over time. There are two particular aspects of endpoint security that are commonly overlooked. Fortunately, both aspects can be clarified by closely considering what requires protection. Ultimately the goal of information security is to ensure the confidentiality, integrity, and availability of the information. It is important to realize that this goal applies regardless of where the associated information resides at any given moment.

Managed versus unmanaged endpoints

The first overlooked aspect is that security must be provided not just for managed endpoints, but also for ones that are unmanaged — endpoints that are beyond your organization's sphere of administrative control, primarily because they're owned by other parties such as employees, business partners, customers, or even the general public.

That managed endpoints need to be secured is relatively clear. Managed endpoints typically have access to a broad range of information and, in many cases, are allowed to retain large portions of it. Of course, not all managed endpoints and their users will have the same rights and permissions, so they will not all require the same set of countermeasures.

In contrast, unmanaged endpoints generally have considerably less access to information compared to managed ones. This reduced access doesn't, however, eliminate the fact that the information is being put at risk. The information could be surreptitiously stored or it could be stolen as a consequence of the unmanaged endpoint having been compromised by some sort of malware. Not having control of the endpoint does impose some significant limitations in terms of what can be done and how it can be accomplished, for example not being able to dictate which types of security controls are persistently installed on the endpoint.

Endpoint security challenges

Securing the endpoints presents some very difficult challenges.

The increased determination and ease with which new threats are being built by malicious parties has not only sparked a dramatic rise in overall threat volume, but it has also reduced the time required for threat development. As a result, the window of time between when a new vulnerability is disclosed and when a specific threat targeting that vulnerability is launched has been greatly reduced.

Yet another challenge stems from the lightning-fast propagation times of today's threats. For example, the Slammer worm achieved an infection doubling rate of 8.5 seconds en route to infecting 90 percent of all susceptible hosts within 10 minutes. The problem with this is that reactive countermeasures can't be updated quickly enough to provide protection during the early phases of new, unknown attacks.

Additionally, threats are increasingly more targeted. Several years ago when an anti-malware signature was updated, typically over 1,000 hosts had seen that particular malware before release. Today, most signatures are created to combat malware that is on only a handful of machines, most often below two dozen machines.

Finally, it is also the case that new threats are more elusive. Blended threats — those that attack on more than one level — are becoming the norm rather than the exception.

The point of all of this is that in order to be considered comprehensive, an endpoint security solution must address the changes in the threat landscape. This means that reactive and other less effective countermeasures must be supplemented with ones that are more proactive, as well as ones that are capable of stopping attacks against higher-layer services.

Securing managed endpoints

Because managed endpoints are within an organization's administrative control, persistent agents can be used to implement necessary countermeasures. Some of these agents include:

- **Local firewall:** A local firewall will allow only traffic that is explicitly allowed by its policy while denying everything else. This approach reduces an endpoint's surface area for attacks by blindly thwarting a wide variety of both known and unknown threats.
- **Application control:** Monitors programs and their libraries to prevent end-users from running applications that could potentially compromise data such as BitTorrent, keystroke loggers, or remote control applications or applications that are malicious in nature.
- **Host integrity checking:** Involves auditing an endpoint to ensure the presence of various attributes such as registry settings that correspond with specific patches, the date on an antivirus signature file, and the presence and version of the antivirus software itself.
- **Patch management:** Patch management is fundamentally about identifying and eradicating weaknesses in software code. And while these are not inherently "bad," vulnerabilities do indisputably enable threats to be effective. Ninety percent of the threats that attack systems propagate through poor patch management practices.
- **Network intrusion protection (host-based):** Similar to a personal firewall, this countermeasure is concerned with network-layer communications and processes and the threats that operate against them.
- **Antivirus:** Focuses on known attacks that are application- and file-based. Advanced antivirus products also incorporate antispyware capabilities, thereby providing protection against nuisance adware as well as more serious threats such as keylogger Trojans.
- **Host intrusion protection:** Provides protection against unknown attacks that operate at the system and application levels as opposed to the network level. The techniques for accomplishing this involve preventing application and operating system behaviors that are either known to be bad or that are dynamically determined to be bad.
- **Buffer-overflow protection:** Also referred to as memory protection, this countermeasure is intended to prevent known and unknown attacks that attempt to exploit poor memory management of applications, using it to gain elevated system privileges.

- **File/disk encryption:** Encryption is effective, particularly for laptops, in the event that the endpoint is physically stolen. In this age of regulatory compliance and heightened sensitivity for data privacy, it is a countermeasure that is increasingly getting attention.

Securing unmanaged endpoints

Compared to managed endpoints, unmanaged endpoints may seem like something that belongs in the Wild West. Because you typically don't have much control over unmanaged endpoints, you have far fewer means of securing them.

Take a look at your options for securing unmanaged endpoints:

- **On-demand host integrity checking:** This is analogous to the host integrity checking countermeasure used on managed endpoints, but the scope of audit capabilities may be somewhat reduced as a result of not having the same system-level rights as a permanently installed agent.
- **On-demand cache cleaning:** Removes information remnants from browser- and application-specific caches upon completion of an access session.
- **On-demand malicious code protection:** Involves identifying keylogger Trojans and other malicious code that may reside on an endpoint, potentially even despite the presence of an antivirus package. Because removal of malware isn't usually possible in an on-demand scenario, the response is limited to blocking access from the infected endpoint.
- **On-demand firewall:** Similar to the managed endpoint firewall, with the exception that it typically involves far fewer connection control capabilities as a result of not operating with full system-level rights.
- **On-demand secure virtual workspace:** Helps ensure against information leakage by creating an encrypted workspace on the endpoint. Typically the workspace and any associated information will be deleted upon completion of the session.

End-user education

No matter how much effort you put into protecting your systems, if you neglect the human factor your results will be disappointing. That's why end-user education is such an important piece of the overall cybersecurity picture.

Symantec strongly recommends that you educate your end-users in the area of professional best practices. Some of these include:

- Don't open unknown e-mail attachments.
- Don't reply to spam; delete all spam.
- Beware of e-mail-based social engineering ploys, such as phishing.
- When sending sensitive information, double-check the addresses to which you are sending the e-mail.
- Don't send or store sensitive information through Web-based e-mail.

Obviously you'll want to greatly expand this list based on your organization's needs, but the important point to remember is that the end-user is a very important part of cybersecurity.

Reporting for Security Incidents

Government agencies typically have much higher logging and reporting requirements than do private companies — especially in the area of security-related incidents. There are, in fact, a set of guidelines that were developed specifically to guide this process.

The *Consensus Audit Guidelines* — or CAG — are aimed at addressing the most effective countermeasures in cybersecurity. A consensus among multiple industry experts, the CAG was developed with the intent to help defend our nation's intelligence and information infrastructures. It reflects 20 key control areas and is a list that resulted from the collaborative work of federal CIOs, CISOs, DoD Blue Team members, FBI cybercrime teams, and forensic experts. The CAG is viewed

as an effective guide for blocking well-known, high-priority attacks across government infrastructures.

The CAG is accompanied by three guiding principles used to develop these 20 control areas and their associated subcontrols. These principles are as follows:

- Defenses should focus on addressing the most common and damaging attack activities occurring today, and those anticipated in the near future.
- Defenses should be automated, where possible, and periodically or continuously measured using automated measurement techniques, where feasible.
- To address current attacks occurring on a frequent basis against numerous organizations, a variety of specific technical activities should be undertaken to produce a more consistent defense.

Tools like the Symantec Risk Automation Suite are designed to help both the implementation of and reporting on the issues addressed by the CAG.

The full list of the Critical Security Controls defined with the CAG can be reviewed at `www.sans.org/critical-security-controls`.

Various Symantec technologies can be utilized to support these Critical Security Controls.

Chapter 3

Looking at the Federal Cybersecurity Guidelines

In This Chapter

- Understanding the federal standards
- Applying non-federal standards and good practices

In recent years it has become clear that cyberattacks can be a major threat against our government and society. There are plenty of bad actors out there who will take any opportunity to try to disrupt our way of life. Fortunately, the federal government has developed guidelines that are designed to help you protect and defend against such threats.

In this chapter, I look at some of those guidelines and also mention some additional resources you can use in your quest for cybersecurity.

Understanding the Federal Standards

The federal government has a lot of computers and it would be virtually impossible to manage all of them without some effective standards and guidelines. The government is, of course, quite adept at developing and publishing rules and regulations, so it should come as no great surprise that there are several of them you need to consider. Take a look at a few very important standards.

Deciphering NIST 800-53A

Almost ten years ago Congress passed the *Cyber Security Research and Development Act,* which directed the National Institute of Standards and Technology — NIST — to develop checklists of settings and options to minimize the security risks associated with the computers used within the federal government. One result of this mandate was a publication called *NIST Special Publication 800-53A, Recommended Security Controls for Federal Information Systems,* which I'll just call *NIST 800-53A* for the sake of brevity.

NIST 800-53A defines a large number of what it calls *baseline security controls.* These baseline security controls are the initial recommended security settings that are based on the system's security categorization. Essentially, *NIST 800-53A* is a set of guidelines designed to help an organization obtain an acceptable level of security in each of a large series of situations.

Effectively, *NIST 800-53A* functions like a large checklist that provides initial security settings for a broad range of scenarios. The broad range of topics defined in *NIST 800-53A* include:

- Access control
- Auditing and accountability
- Awareness and training
- Certification, accreditation, and security assessments
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical and environmental protection
- Planning
- Risk management

- System and communications protection
- System and information integrity
- System and services acquisition

Each of these main topics has up to 23 subtopics, depending on the controls that are addressed by the topic. You can find the latest revision of *NIST 800-53A* at `csrc.nist.gov/publications/PubsSPs.html`.

Getting to the core of FDCC

The next set of guidelines I'll examine is the *Federal Desktop Core Configuration*, or FDCC. The FDCC is a mandate from the U.S. Office of Management and Budget (OMB) that requires all Federal agencies to standardize the configuration of about 300 settings on each of their PCs. The intent of the mandate is to improve security by making certain the systems are properly configured to resist cyberattacks.

The FDCC currently mentions PCs that use Windows XP or Windows Vista, but not Windows 7, Macintosh, or Linux. If you're configuring a Windows 7–based PC, most of the Windows Vista settings will apply. But if you're configuring a Mac or a Linux system, you're on your own.

A few of the more visible effects of FDCC include:

- Passwords must be changed every 60 days.
- User logins are not saved so users are required to enter both their username and password each time they log on.
- Users aren't allowed to have administrator privileges unless they are granted a special waiver.
- Many applications may not work properly because of users not having administrator privileges.
- All wireless connections are supposed to be disabled (but some agencies such as the National Institutes of Health allow wireless access in spite of FDCC).

The FDDC is updated from time to time as NIST continues its development of the standard. To get the latest information on FDCC visit `nvd.nist.gov/fdcc/index.cfm`.

The FDCC is being replaced by the United States Government Configuration Baseline (USGCB). The United States Government CIO council has issued direction on the USGCB at `www.cio.gov/Documents/USGCB_CIOC091510_final.pdf`.

Both the FDCC and the USGCB were developed as security baselines across a limited set of operating systems. These are not intended to replace a holistic security policy.

Reporting with SCAP

The final federal guideline I'll look at is the *Security Content Automation Protocol* (or SCAP) — a method for enabling automated vulnerability management, measurement, and policy compliance evaluation. SCAP was intended to standardize a number of security-related issues so that products from different vendors could work together.

There are actually six standards which make up SCAP:

- **Common Vulnerabilities and Exposures (CVE):** A dictionary of names for publicly known security related software flaws.
- **Common Configuration Enumeration (CCE):** A dictionary of names for software security configuration issues, such as access control settings and password policy settings.
- **Common Platform Enumeration (CPE):** A naming convention for hardware, operating systems, and software.
- **Common Vulnerability Scoring System (CVSS):** A method for classifying characteristics of software flaws and assigning severity scores.
- **Extensible Configuration Checklist Description Format (XCCDF):** An Extensible Markup Language specification for structured collections of security configuration rules used by operating systems and applications.
- **Open Vulnerability and Assessment Language (OVAL):** An XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and patches.

The essential value of SCAP comes from standardizing the terms used to describe security issues. This standardization means that each vendor uses the same names for security threats and is also supposed to assign the same priority to each problem. As a result, agencies aren't confused by duplication of efforts trying to fix the same problem appearing under different names. In addition, the CVSS component of SCAP should mean that it is easier to determine just how critical a threat may be.

You can find the latest information on NIST's SCAP initiative at `scap.nist.gov`.

Additionally, the latest reporting initiative within the US Government, CyberScope, has been defined to provide agencies with better FISMA reporting within the SCAP initiative. For more information, go to `http://scap.nist.gov/use-case/cyberscope/index.html`.

Applying Non-Federal Standards and Good Practices

Although the federal guidelines and standards address a broad range of cybersecurity issues, almost everyone would agree that there are many other good ideas that come from outside the government. For example, Symantec has identified five keys to protecting sensitive information. Take a look at these five keys.

Accuracy is mission-critical

To be successful, you must accurately detect every single security policy violation, whenever, wherever, and however it occurs. Most content monitoring solutions only yield approximate identifications, resulting in frequent false alarms and unnecessary fire drills, while undetected data continues to flow out through the network. Make sure the software vendor you choose delivers the highest degree of accuracy, with no false positives.

E-mail is only a portion of the problem. Research shows that 50 percent of incidents occur via Internet protocols other than e-mail. Your solution should accurately monitor and detect security violations for all data types, all data endpoints (removable media, network activities, copy/paste, and print/fax), and all network protocols, including e-mail (SMTP), instant messaging (AOL, MSN, Yahoo!), Web, secure Web (HTTP over SSL), FTP, P2P, and generic TCP sessions over any port.

Don't just monitor violations, stop them before they occur

It's not enough to simply track security violations; the key is to prevent them from happening before the horse is out of the proverbial barn. Make sure your solution can stop transmissions that violate security, acceptable use, and privacy policies before they leave the network. Many organizations elect to begin with monitoring and then expand to prevention. Your software vendor should provide a development path that allows you to grow the solution over time.

Time is of the essence

When information security violations occur, it is essential that you respond immediately. Rapid response can mean the difference between safe and sorry.

Regulations such as the Federal Information Security Management Act (FISMA), White House Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST) PII Requirements, and the National Infrastructure Protection Plan (NIPP) require immediate response to information security breaches regardless of whether they involve classified information. You need immediate, actionable information and process automation to enable rapid response.

Your software vendor's solution should provide real-time alerts, customizable workflow, and a complete profile of each incident — including content, sender, recipient, timing, and policy information. It should also automatically identify and notify the sender.

You can't manage what you can't measure

Monitoring data loss incidents is only the first step. To meet your security and compliance goals, you need to measure the effectiveness of your information security plan over time, so you can weigh risks, fix broken processes, and identify potential compliance issues.

Your software vendor's solution should deliver centralized, one-click reporting that covers all the multiple exits and endpoints on your network. Users should be able to easily aggregate data, drill down on details, and distribute reports, including historical trend analysis, investigative forensics, and regulatory compliance.

Make information security a department- or agency-wide initiative

To elevate information security to a higher strategic priority, you need to educate employees about applicable information security regulations and enable staff at every level of your organization to actively participate in the protection of sensitive as well as classified information.

Your software vendor's solution should be tailored to the business/process user. Look for role-based access control to enable business units to review and remediate only those incidents relevant to their roles and privileges. Look also for executive dashboards that present the big picture for senior management. Ensure that you can do reporting by functional unit to support benchmarking and accountability.

Manage the data

An effective security policy must incorporate the appropriate methods for data assurance and management. As previously discussed, the actual systems are used to gain access to your data. Preventing the loss of data is very critical to any security program.

Chapter 4

Examining Symantec's Cybersecurity Ecosystem

In This Chapter

- Using desktop- and server-focused solutions
- Applying network-focused solutions
- Making reporting easier

Security threats make good cybersecurity important. You need reliable solutions as well as knowledgeable partners as you develop your plans to meet the cybersecurity needs of your organization.

In this chapter, I look at how Symantec and its partners provide the solutions you need as well as the expertise to ensure that you get the correct set of products for your specific situation.

Using Desktop- and Server-Focused Solutions

It's important to apply the correct types of protection for your organization so that there won't be any gaps waiting to be exploited (for more on this, see Chapter 2). In this section, I take a look at Symantec's endpoint protection solutions that can help protect your desktops and servers.

Compliance

Every government organization has to comply with a number of different regulations. Compliance can be a major headache unless you have the proper policies and procedures in place so that any technical solutions can correctly enforce them.

Symantec Control Compliance Suite is the only fully automated solution to manage all aspects of IT risk and compliance at lower levels of cost and complexity. Control Compliance Suite offers out-of-the-box content on multiple industry regulations, automated assessment of technical and procedural controls, Web-based dashboard reporting, and integration with other Symantec security solutions.

Endpoint protection/Critical systems protection

Providing proper security for all your endpoints is both critical and complex. The task is made even more difficult when you have a mix of managed and unmanaged endpoints as discussed in Chapter 2, because you have far less control over the unmanaged endpoints than you do over your managed endpoints.

Ultimately, the goal of information security is to ensure the confidentiality, integrity, and availability of sensitive or valuable information. This goal applies regardless of where the information resides. An ideal endpoint security solution is one that provides protection of and from both managed and unmanaged hosts, against both known and unknown attacks.

If possible, you want a solution that prevents intrusions and stops attacks quickly, has advanced capabilities so it can deal with previously unknown threats, and which provides you with useful information about any attacks in a clear and timely manner.

Symantec offers a range of suites and products that meet these needs:

- **Symantec Protection Suite Enterprise Edition** creates a protected endpoint, messaging, and Web environment that is secure against malware, data loss, and spam threats.

- **Symantec Protection Suite Enterprise Edition for Endpoints** manages the business risk of IT by reducing the risk profile of your most frequently targeted and attacked assets.
- **Symantec Protection Suite Enterprise Edition for Servers** protects against physical and virtual server downtime with policy based prevention using multiple protection technologies combined in a single protection suite with flexible controls against known and unknown vulnerabilities. The following products are contained within the suite:
  - **Symantec Endpoint Protection 11.0** combines Symantec AntiVirus with advanced threat prevention against malware for laptops, desktops, and servers.
  - **Symantec Network Access Control 11.0** securely controls access to networks, enforces endpoint security policy, and easily integrates with existing network infrastructures.
  - **Symantec Critical System Protection 5.2** protects against zero day attacks, hardens systems, and helps maintain compliance by enforcing behavior-based security policies on clients and servers.

In addition to these products, Symantec offers a couple of endpoint security services that may meet your needs. Using one of these services can make your life a little easier because you have dedicated and knowledgeable experts there to help you:

- **Endpoint Security Services** helps to ensure the stability, performance, and scalability of the Symantec Endpoint Protection and Symantec Network Access Control technologies through a number of different means.
- **Symantec Hosted Endpoint Protection** offers comprehensive security for Windows-based laptops, desktops, and file servers as a hosted service without installing additional hardware or management software.
- **Symantec Managed Endpoint Protection Services** deliver prevention against threats by combining endpoint protection solutions with 24 x 7 remote monitoring and onsite management by security experts.

Of course these very brief descriptions don't really give much of the story about the Symantec endpoint security solutions. You can visit `www.symantec.com/business/solutions/solutiondetail.jsp?solid=sol_security&solfid=sol_endpoint_security` for additional information.

Endpoint encryption

The endpoint security solutions mentioned so far have focused on preventing or mitigating various types of attacks on your systems. The solution discussed in this section serves a different purpose — it protects the data that is contained on those systems in the event someone is able to steal one of them.

Over the past several years there have been a number of high-profile incidents where a user has lost a laptop, a hard drive, or a removable storage device that contained highly sensitive or classified information — and probably many more incidents that went unreported! Laptops, portable hard drives, and USB keys are quite easy to carry around and they're extremely easy to steal or just misplace. They're also much sought after by criminals who have no trouble turning a profit on them.

But when one of your users loses one of these highly portable devices, they've lost far more than simply an expensive piece of hardware — because, without encryption, any information contained on the device is there for the taking. Depending on the nature of the lost information, there could be a whole raft of nasty people who would be very happy to get their hands on it.

Symantec Endpoint Solutions (Symantec Endpoint Encryption and PGP) provides advanced encryption for e-mail, servers, desktops, laptops, and removable storage devices using strong access control and powerful military-grade encryption. By making it impossible to access any of that sensitive information without the proper credentials, Symantec Endpoint Solutions might just make it a little easier for you to sleep knowing that your name isn't going to be front-page news for allowing the bad guys access.

Applying Network-Focused Solutions

In addition to endpoint-focused cybersecurity solutions, an organization needs solutions that can control network level attacks. Network-focused cybersecurity tools provide advanced content filtering, data loss prevention, and e-mail encryption to control sensitive data, reduce data loss, and meet regulatory compliance demands.

The following sections take a closer look at some of the relevant network-focused cybersecurity tools from Symantec.

Brightmail Gateway

Symantec's Brightmail Gateway provides inbound and outbound messaging security, real-time antispam and antivirus protection, advanced content filtering, data loss prevention, and e-mail encryption.

Brightmail Gateway catches more than 99 percent of spam with less than one in a million false positives. The product uses real-time automatic antispam and antivirus updates, on-box connection throttling using both global and self-learning local IP reputation, and on-demand reporting, unified administrative controls, and flexible work flow.

With Brightmail Gateway, organizations can effectively respond to new messaging threats, minimizing network downtime, preserving employee productivity, and protecting company reputation. Advanced content filtering, data loss prevention, and e-mail encryption help organizations control sensitive data, reduce the risks associated with data loss, and meet regulatory compliance and corporate governance demands.

One feature of Brightmail Gateway that is of special interest to governmental organizations is outbound control of sensitive data flow, which helps enforce regulations. Brightmail Gateway features advanced content filtering and data loss prevention technologies that make it easier to protect and control sensitive data. You can easily build effective and flexible policies that enforce regulatory compliance and

protect against data loss. Techniques like keyword and regular expression scanning inside messages and attachments help you gain control over messaging content and comply with regulations. You can create policies that enforce encryption or "Hold for Review" before allowing message delivery, providing an opportunity for administrative intervention by compliance staff if needed.

This discussion has only touched the surface of Brightmail Gateway. For additional information see `www.symantec.com/business/brightmail-gateway`.

Traffic Shaper

The Symantec Brightmail Traffic Shaper is a component of the Brightmail Gateway. Brightmail Traffic Shaper is a hardware appliance that reduces total e-mail volume by up to 70 percent and cuts spam volume by up to 80 percent or more before it reaches the Brightmail Gateway or another vendor's antispam solution.

Brightmail Traffic Shaper controls spam volume before it enters the network while ensuring the continuous flow of legitimate mail. This reduction in spam volume significantly reduces administrative overhead, network bottlenecks, and reduces mail infrastructure costs. The appliance processes e-mail traffic at the TCP layer prohibiting spammers from forcing mail into a protected network.

Some of the key features and benefits of adding the Brightmail Traffic Shaper include:

- Reduces up to 80 percent of spam volume before it impacts the network and e-mail infrastructure, while ensuring the continuous flow of legitimate mail.
- Contains escalating mail infrastructure costs and lowers administrative hardware, storage, and network overhead caused by the exploding spam volume.
- Shapes traffic at the TCP protocol level by assigning resources to good senders and reducing the quality of service (QoS) available to spammers. This causes mail to back up on the spammers' servers without having to block legitimate incoming mail.

- Easy to install, compatible with any messaging server, and operates transparently in the network.
- A single appliance handles up to 750,000 user accounts and can process thousands of messages a second, depending on the message size.

To find out more about Brightmail Traffic Shaper, visit `www.symantec.com/business/brightmail-traffic-shaper`.

Mail Security for Exchange/Domino

If your organization has its own Microsoft Exchange or Lotus Domino mail server, you need real-time protection against a whole raft of attacks. Symantec Mail Security for Microsoft Exchange and Symantec Mail Security for Domino Multi-Platform Edition are the products that can supply that protection.

Both of Symantec's Mail Security products are based on Brightmail technology and both offer similar features such as real-time protection against viruses, spam, spyware, phishing, and other attacks while enforcing content policies for your e-mail, documents, and databases. Symantec Mail Security complements other layers of protection by preventing the spread of e-mail-borne threats internally and by serving as a first line of defense.

Some of the key benefits of using one of the Symantec Mail Security solutions include:

- Provides real-time protection against viruses, mass mailer worms, Trojan horses, spam, spyware, phishing, and denial of service attacks
- Enforces content policies
- Powered by Brightmail technology, stopping 99 percent of spam while making fewer than one mistake per million messages
- Rapid release definitions and proactive signature independent technologies provide immediate protection
- Advanced Content Filtering protects sensitive information using predefined policies, regular expressions, attachment criteria, True File typing, and more

- Supported by the largest investment in infrastructure with a security R&D team that is 50 percent larger than the closest competitor
- Initial setup can be completed within ten minutes, with no requirements for tuning, allow listing, or block listing
- Management console provides centralized server group policy configuration, notifications, alerts, and reporting
- Support for Database Availability Group minimizes downtime and simplifies maintenance
- Flexible real-time, scheduled, and manual scanning provides efficient protection
- In-memory scanning and effective multi-threading provides superior performance

You can find out more about Symantec Mail Security for Microsoft Exchange at `www.symantec.com/business/mail-security-for-microsoft-exchange`.

You can find out more about Symantec Mail Security for Domino at `www.symantec.com/business/mail-security-for-domino`.

Making Reporting Easier

As discussed in Chapter 3, government organizations have strong and well-defined guidelines for managing and reporting on security-related issues. In the following sections I discuss two tools designed specifically to meet these guidelines — the Symantec Risk Automation Suite and the Symantec Security Information Manager.

Risk Automation Suite

The Symantec Risk Automation Suite is designed to enable automated and integrated vulnerability management, measurement, and policy compliance evaluation as called for in the NIST Secure Content Automation Protocol (SCAP).

The Symantec Risk Automation Suite helps organizations continuously discover and visualize all IT networks and assets, prioritize risk accordingly, and measure remediation efforts

for the most complete, accurate, repeatable risk assessment of the IT environment. Risk Automation Suite has received the following SCAP validations from NIST:

- Federal Desktop Core Configuration (FDCC) Scanner — able to audit and assess target systems for FDCC compliance and reporting; has options included for agent-less, dissolving-agent, or persistent-agent scanning
- Authenticated Configuration Scanner — able to audit and assess target systems for compliance with defined configuration requirements
- Authenticated Vulnerability and Patch Scanner — able to scan target systems to locate and identify software flaws and evaluate patch status and compliance with patch policy
- Common Configuration Enumeration (CCE)
- Common Vulnerability Scoring System (CVSS)

Risk Automation Suite automatically measures IT security and compliance for standards such as the following:

- Federal Information Security Management Act (FISMA)
- Federal Desktop Core Configuration (FDCC)
- Certification and Accreditation (C&A)
- NIST 800 Series (NIST 800-53r3)
- Health Insurance Portability and Accountability Act (HIPAA)

You can learn more about the Symantec Risk Automation Suite at `www.symantec.com/business/risk-automation-suite`.

Security Information Manager

One very important requirement for many government organizations is monitoring and reporting on security-related events. Meeting this requirement can be a very difficult task unless you're equipped with the proper tools that are specially designed for the job.

Symantec Security Information Manager enables you to collect, store, and analyze log data as well as monitor and respond to security events to meet IT risk and compliance

requirements. It can collect a broad range of event data and correlate the impact of incidents.

With Symantec Security Information Manager, incidents are prioritized using a built-in asset management function. In addition to establishing priority to events, Symantec Security Information Manager can provide for response and remediation efforts. Automated updates from Symantec's Global Intelligence Network provide real-time information on the latest vulnerabilities and threats that are occurring across the rest of the world.

Symantec Security Information Manager can enable you to produce executive, technical, and audit-level reports that are highly effective at communicating risk levels. Over 300 out-of-the-box queries can create custom reports. Security Information Manager automates the real-time collection, monitoring, and assessment of audit mechanisms and security controls and can dramatically lower costs and improve the effectiveness of managing activities related to IT security and compliance risks.

Symantec Security Information Manager addresses some important security and compliance challenges that you are likely to face:

- **Understanding security posture and meeting audit standards:** Symantec Security Information Manager is a real-time security information management solution that collects, correlates, and stores event, vulnerability, and compliance logs and documents the actions that your security staff takes to help keep your information systems secure. It provides compliance reporting that lets you and your auditors see, firsthand, the state of your security environment. These are crucial to helping your organization provide the accountability and transparency required to comply with stringent mandates and regulations.
- **Assessing threats and security issues:** Symantec Security Information Manager allows you to identify the threats you are most vulnerable to and provides remediation steps to address those threats in real time. It will also classify threats and security issues as they occur based on the effect those events will have on your environment.

- **Identity and access management:** Symantec Security Information Manager can leverage information from existing security and compliance products to assist in monitoring identity and access activities. It can help you gain visibility into user access of systems and produce audit trails showing access and changes to critical applications and assets.

You can find out more about Symantec Security Information Manager at `www.symantec.com/business/security-information-manager`.

Chapter 5

Top Ten Cybersecurity Suggestions

In This Chapter

- Knowing not to open attachments
- Understanding how to be careful

Once in a while it helps to be reminded of some important things that will help protect you and your systems. In this chapter, I take a very quick look at some cybersecurity suggestions that will help keep you safe.

- Don't open unknown or unexpected e-mail attachments even if they appear to come from someone you know.
- When sending sensitive information, double-check the addresses to which you send the e-mail and be sure that you aren't sending confidential information to third parties unless they're authorized to receive the information. Don't send or store sensitive information through Web-based e-mail.
- Be selective about the Web sites with which you register your e-mail address or provide any other personally identifiable information.
- Always use the latest virus protection, with the latest updates and make sure your operating system and third-party applications patches are updated, too.
- Beware of e-mail-based social engineering ploys, such as phishing. Fake Web sites can appear quite real — when there is any question about the validity of a message, enter the URL manually rather than clicking a link in a message.

- If anyone requests your login information via e-mail, don't provide the information. Rather, report the request to the IT Service Desk immediately.
- Never share or write down your passwords where others may access them. Passwords must not contain the username and must not be based on personal information, such as family names.
- Protect your laptop and PDA against loss or compromise. Never leave your laptop or PDA in plain view and unattended, and obtain a privacy screen if you travel or work with sensitive information.
- Don't reply to spam; delete all spam. Never click an unsubscribe link in a spam message.
- If you use Instant Messaging (IM), don't share sensitive or confidential information via IM and always use the latest versions of IM software as older versions may have security flaws.

SYMANTEC
PROTECTS MORE

THAN ANYONE.

Learn more: www.securityleader.com

Symantec™ DLT SOLUTIONS

www.dlt.com/brands/symantec/security • 888-472-4358

Find out all about cybersecurity and how it can help government organizations

Cybersecurity For Dummies, Symantec and DLT Solutions Special Edition, shows you the threats that make securing your systems so important. You'll see some of the trends that show where cyberthreats are headed and the multiple layers that must be protected.

- ***Cybersecurity basics* — find out why and how your information is at risk from cybercriminals**
- ***Looking at layered defenses* — different layers of your computing environment need their own, targeted types of protection**
- ***Federal guidelines* — take a look at the important federal standards that you must follow to keep your cybersecurity efforts in compliance**
- ***Symantec cybersecurity solutions* — Symantec products can make your life easier by providing the cybersecurity solutions you need**

Open the book and find:

- **Information on desktop, server, and network-focused solutions**
- **A list of suggestions to follow to make your cybersecurity solution the best it can be**
- **How to work with federal guidelines**
- **Where to find info on how to log and report security incidents**

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

For Dummies®
A Branded Imprint of
WILEY

978-1-118-01137-9
Not for resale