realtimepublishers.com™

The Definitive Guide™ To

Controlling Malware, Spyware, Phishing, and Spam

McAfee®
Proven Security™

Dan Sullivan

Introduction to Realtimepublishers

by Sean Daily, Series Editor

The book you are about to enjoy represents an entirely new modality of publishing and a major first in the industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical technology topics—at no cost to the reader. Although this feat may sound difficult to achieve, it is made possible through the vision and generosity of a corporate sponsor who agrees to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these publications does not in any way diminish their quality. Without reservation, I can tell you that the book that you're now reading is the equivalent of any similar printed book you might find at your local bookstore—with the notable exception that it won't cost you $30 to $80. The Realtimepublishers publishing model also provides other significant benefits. For example, the electronic nature of this book makes activities such as chapter updates and additions or the release of a new edition possible in a far shorter timeframe than is the case with conventional printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that our books are by no means paid advertisements for the sponsor. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100 percent editorial control over the content of our titles. It is my opinion that this system of content delivery not only is of immeasurable value to readers but also will hold a significant place in the future of publishing.

As the founder of Realtimepublishers, my *raison d'être* is to create "dream team" projects—that is, to locate and work only with the industry's leading authors and sponsors, and publish books that help readers do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please send an email to feedback@realtimepublishers.com, leave feedback on our Web site at http://www.realtimepublishers.com, or call us at 800-509-0532 ext. 110.

Thanks for reading, and enjoy!

Sean Daily
Founder & Series Editor
Realtimepublishers.com, Inc.

Introduction to Realtimepublishers.. i
Chapter 1: Overview of Preventing Malware, Spyware, Spam, and Phishing Scams.....................1
Proliferation of Internet Content and the Roles of Internet Content in Organizations 2
Organizational Responsibilities for Securing the IT Environment...4
Protection of Information Assets 4
Systems Infrastructure 5
Core Applications and Supporting Software 5
Protecting Data...9
Efficient Operations...10
Non-Threatening Work Environment..11
Protecting Against Loss of Controlled Information...11
Regulatory Compliance 12
Compliance and Security 13
Summary of Organizational Responsibilities 13
Threats Posed by Internet Content..14
Viruses, Worms, Trojan Horses, and Other Malware..14
Computer Viruses 14
Worms...16
Trojan Horses..16
Additional Forms of Malware..17
Spyware...17
Phishing..18
Spam 19
Undesirable Web Sites..19
Countermeasures to Threats..20
Content Filtering 20
URL Filtering..20
Antivirus Software 21
Anti-Spyware 21
Spam Management...21
Countermeasure Implementations 22
Summary 22

Copyright Statement

[**Editor's Note:** This eBook was downloaded from Content Central. To download other eBooks on this topic, please visit http://www.realtimepublishers.com/contentcentral/.]

Chapter 1: Overview of Preventing Malware, Spyware, Spam, and Phishing Scams

The Internet is a double-edged sword. It is fundamental infrastructure for contemporary businesses and organizations—the Internet has evolved from research tool to the basis for more efficient production and better distribution of information. We have all benefited from new services such as virtual marketplaces and online comparison shopping to instant access to wide ranges of information from a single search engine. However, while realizing these benefits, we have also opened ourselves and our systems to a number of threats.

The Internet is home to malicious programs that can steal, destroy, and make data inaccessible; spyware that ignores social conventions of privacy to track Internet users' activities online; phishing scams that bring the art of the con artist to new threatening levels; and spam, the inevitable electronic counterpart to direct mail that requires so little investment even miniscule response rates justify its use. Consider just a few examples:

- Phishers have claimed to represent Citibank, SunTrust, and Bank of America with emails to customers notifying them of alleged attempts to log on to online accounts from foreign countries or the need to update customer information.
- Brilliant Digital Entertainment has embedded spyware in the popular Kazaa file sharing program to track users' online activities as well as to add infected PCs to a distributed network controlled by the company.
- Spammers claiming to be relatives of deposed government officials in politically unstable countries promise millions of dollars in return for an advance fee to help the alleged victim flee their country. These are known as 419 frauds after the section of the Nigerian criminal code that makes such spam messages illegal.

Imagination is the only limit on the types of fraud and misappropriation of computing resources that arise on the Internet.

📖 For more details about these and other threats, see "Stealth P2P network hides inside Kazaa" at http://news.com.com/2100-1023-873181.html, the anti-phishing Web site at http://www.millersmiles.co.uk/, and the spam archive at http://www.spamarchive.org/. Expert Law has a good layman description of email frauds at http://www.expertlaw.com/library/consumer/spam_email_fraud2.html.

Proliferation of Internet Content and the Roles of Internet Content in Organizations

Although Internet threats abound, the value of standardized, cross-organization, distributed computing is so great that organizations find it too compelling to ignore. For example, many services we take for granted are built on Internet services:

- **Email—**Email is now a standard means of communications within and between organizations. Its advantages—such as low cost, broad and rapid distribution, and electronic copies that can be stored for long periods of time—make it a superior method of communications compared with telephones and postal mail.
- **E-commerce—**Businesses and organizations find what they need faster and with greater options because of online catalogs and ordering, customer self-services, virtual marketplaces, comparison shopping sites, and online consumer reviews.
- **Workflow—**Complex business processes are routinely broken down into smaller steps, and workflow software allows greater control and efficiency than possible in the past. Some of the benefits provided by workflow software include:
    - Embedded business logic that can automatically control the flow of information and tasks
    - The ability to distribute work tasks anywhere in the world, which allows businesses to find the optimal combination of cost and quality
    - Process management and reporting, which provide managers with data on the status of production throughout complex business operations

The Internet has become the foundation of services and operations to the point that we can think of it as a utility, like electric and water services, but with some challenging differences.

The Internet: A New Kind of Infrastructure

Clearly the Internet has demonstrated its value as well as its potential dangers. As with other kinds of infrastructure, we need to set up the Internet to maximize benefits and minimize dangers. Take electricity for example. Does anyone think twice about plugging an appliance into an outlet? We assume the electricity will be available at the proper voltage and amps to run the appliance without damaging it. Most of us know the basics of how power is generated and transmitted, and some are familiar with how power companies adjust the load on the electrical grid to keep meeting demand without overloading the system. Except for engineers in the industry though, the vast majority of electric users do not know the subtle nuances and technical details of how that supply and demand balance is met. Nonetheless, we can all work a toaster. The electrical system in fully industrialized countries has matured to the point where we can use it reliably and consistently without having to worry about a lot of technical details.

Similarly, while most Internet users understand the basics of networking, they do not have to concern themselves with the idiosyncrasies of protocols, routers, and servers. Unlike the electric grid, however, the Internet cannot be trusted to function as expected in all cases. If the Internet were used as benignly envisioned by most, users would be fine. Unfortunately, electronic utopias are no more real than social ones. The analogy between the electric grid and the Internet breaks down in two key ways.

- **Openness—**First, unlike the electric grid, which has relatively few producers able to substantially alter its state, the Internet is open to all.
- **Complexity—**Second, the network is more complex; the Internet communicates instructions and data around the world, it does not just transmit energy in a narrowly controlled manner.

This combination of openness and complexity is the underlying reason for both the Internet's benefits and its threats.

> If you are not convinced a single person could substantially affect the Internet, read about the effects of SQL Slammer, a malicious program known as a worm that spread so rapidly that Internet traffic was effectively shut down within minutes of the program's release. For more information about this worm, see CNN's "Computer Worm Grounds Flights; Blocks ATMs" at http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/ and CNET's "Slammer Attacks May Become Way of Life for Net" at http://news.com.com/Damage+control/2009-1001_3-983540.html.
>
> For a high-level summary of how the Internet and related technologies have changed businesses and organizations, see Thomas Friedman's *The World is Flat: A Brief History of the Twenty-First Century*, (Farrar, Straus and Giroux, 2005).

This guide explores some of the most pressing threats to businesses and organizations from the Internet along with best practices for addressing them. Chapter 1 presents an overview of the problem and includes:

- Organizational responsibilities for securing the IT environment
- Threats posed by Internet content
- Countermeasures to threats
- Countermeasure implementations

Chapter 2 examines what organizations can do to protect employees, customers, stakeholders, and information assets from the malicious elements on the Internet. In Chapter 3, the topic turns to viruses, worms, and an especially virulent combination of malware known as blended threats. Chapter 4 addresses how to control spyware in the enterprise with detailed explanations of different types of spyware, how it works, and what can be done to control it. Phishing and identity theft are covered in Chapter 5. This chapter includes a discussion of the structure of a phishing attack, it objectives, the economics of phishing, and, of course, how to reduce the incidents of successful phishing attacks. In Chapter 6, the focus is on spam with an emphasis on managing spam and evaluating the effectiveness of anti-spam systems. Chapter 7 takes a comprehensive look at technologies for securing users and information assets from the threats described throughout the guide, then describes best practices for controlling threats from Web and email content. Finally, Chapter 8 presents an overview of some of the implementation options available for controlling malware, spyware, spam, and phishing. The chapter concludes with best practices for a comprehensive approach to securing an internal network from external, Internet threats. The goal of this book is to provide you with the tools needed to leverage the benefits of the Internet with the most safety and reliability possible.

Organizational Responsibilities for Securing the IT Environment

Every organization that uses the Internet has some responsibility for protecting itself from the potential damage to information assets and harm to users. The main areas of concern are:

- Protection of information assets
- Efficient operations
- Non-threatening work environment
- Protecting against loss of controlled information
- Regulatory compliance

Some of these concerns are relevant to all organizations, such as protection of information assets, while others, such as regulatory compliance, will require varying levels of attention depending upon the specific nature of your business.

Protection of Information Assets

One of the most obvious concerns to business users of the Internet is protecting their information assets, in particular:

- Systems infrastructure
- Core applications and supporting software
- Data

Each type of asset has its own particular set of needs with regards to preserving the integrity of the asset.

Systems Infrastructure

Systems infrastructure consists of the servers, desktops, laptops, mobile devices, and networking hardware that comprise the organization's information systems hardware. The greatest threats to hardware are physical: damage from fire, flood, storm, and other natural disasters. For the most part, these threats are best dealt with through appropriate disaster recovery and business continuity planning. The main threats from the Internet target the software running on these machines and the data stored on them.

> 📖 For more information about disaster recovery and business continuity planning, see "The Disaster Recovery Guide" at http://www.disaster-recovery-guide.com/ and the SANS Infosec Reading Room on disaster recovery at http://www.sans.org/rr/whitepapers/recovery/. For up-to-date news on severe weather warnings, see the United States National Oceanic and Atmospheric Administration (NOAA) National Warning Web site at http://iwin.nws.noaa.gov/iwin/nationalwarnings.html.

Core Applications and Supporting Software

Core applications are programs that support an organization's primary activities. They are as diverse as the businesses, governments, and other organizations that use them. For example:

- An enterprise resource planning (ERP) system controls a manufacture's inventory, production, and distribution operations
- Claims processing systems are used by insurers to store, review, and pay claims
- Sales force automation systems track contacts, proposals, contracts, and other material needed by sales teams
- Emergency responders use computer-aided dispatch systems to manage police, fire, and ambulance services

When core applications are down, the organization's ability to function is severely hampered. Large businesses and organizations can often support contingency servers with backup applications that can be quickly brought online in the event of a failure of the primary systems. For small and midsized businesses, fully functional contingency servers may be too costly to justify. In those cases, it is even more imperative to minimize the threats to those core applications.

Threats to Core Applications

Major threats to core applications are not necessarily directed against those applications themselves. There are certainly cases in which it would be worth an attacker's effort to target a large application with few implementations (for example, military and intelligence systems or electronic check and credit card clearing house applications). Although the number of targeted attacks against specific businesses, such as the major attack on the credit card transaction processor, CardSystems Solutions (http://www.computerworld.com/databasetopics/data/story/0,10801,102631,00.html), can be expected to increase, many current attacks target supporting software at the operating system (OS) and networking level. These attacks are not against the core application itself (for example, the ERP system), but they can effectively damage and disrupt the core application as if it had been a direct attack.

> 📖 For more information about a targeted attack to a core application, see "Hackers Using Targeted Attacks to Steal Firms' Customer Data" at http://www.ccnmag.com/news.php?id=3633.

Threats to Supporting Systems

Vulnerabilities in OSs and network software are widely known and, in some cases, easily detected. Hacking tools, such as vulnerability scanners, are readily available on the Internet, along with other tools, such as root kits, which allow even beginner hackers to take control of servers, desktops, and other devices connected to the Internet. In fact, most of the top vulnerabilities in Windows and UNIX environments, target OS and networking systems, including:

- Web servers and services
- Web browsers
- File sharing
- Mail clients
- BIND domain name service
- Simple Network Management Protocol (SNMP)

Databases, which are ubiquitous in enterprise-level applications, are so complex that they too suffer from security vulnerabilities. Widely used databases—including Microsoft SQL Server, Oracle, MySQL and PostgreSQL—have all had vulnerabilities that allow the databases to be compromised.

> 📖 For details about these and other top vulnerabilities, see the SANS' list of top vulnerabilities, "The Twenty Most Critical Internet Security Vulnerabilities" at http://www.sans.org/top20/.

When systems are connected to the Internet, they are exposed to threats that exploit vulnerabilities in core applications and supporting software. It is essential that systems administrators and IT managers keep applications and OSs patched to minimize the chance of a security breach.

In addition, IT staff responsible for infrastructure must understand that patching vulnerabilities and subscribing to OS update services is not enough to secure systems. First, a vulnerability may be discovered and exploited by an attacker before it is known to the application developers who could correct the flaw with a patch.

In addition, the process of testing and deploying patches can be time consuming, especially in large organizations. Change control procedures must be followed when applying patches just as they are when implementing any other change to software. These procedures typically include determining whether the patch is necessary (there is no need to apply a patch for a system service that is not used), whether the patch functions correctly in your environment (many systems administrators have applied OS service packs only to find they break critical applications), and how to deploy the patch (deployment must be prioritized so that the most critical of the vulnerable servers are patched first).

Addressing vulnerabilities is one piece of a broader security profile that must be in place to protect information assets. Access controls (to prevent disgruntled employees from damaging applications from within, for example) and Internet content management (such as antivirus, anti-spam, anti-spyware, and anti-phishing software) are also essential elements.

Beyond Vulnerability Management

Vulnerabilities in systems can only be exploited if a program or a person gains access to the vulnerable system. Some methods of entry are:

- Attaching viruses to email messages that are passed through firewalls directly to email servers
- Launching worms from ActiveX components running within an Internet Explorer (IE) browser
- Probing for open ports on firewalls and exploiting a known vulnerability (SQL Slammer spread this way)
- Using a virus or leaving a malicious program on a computer that then listens for instructions for a specific chat room or other two-way communication method

In an ideal world, these various forms of malware would never make it past network perimeter defenses. The real world is too complicated. Some ports have to be left open on firewalls, some applications depend on browser-based applets, and email systems are designed to move and distribute large quantities of content across secure boundaries. In addition to blocking some network traffic at the perimeter, you must also examine the content that pass through the perimeter to ensure it is not carrying a malicious payload.

Where Is the Network Perimeter?

The concept of a network perimeter is changing as we deploy ever more sophisticated distributed applications. Web services, for example, is a framework for building applications that take advantage of computing services on any accessible server that is using standard Internet protocols. Consider an online book seller who takes orders using a local order management system that calculates state- and country-specific sales tax using a third-party Web service. The system also determines shipping costs and delivery dates using a Web service provided by the book seller's shipping company. Where is the book seller's network perimeter?

The purchaser is certainly outside the perimeter; other than the occasional book orders, this person's system has no long-term, well-defined links to the seller's systems. Technically, Web services from third parties are outside the control of the book seller and therefore outside the network perimeter. Yet, these services are essential to the business operations of the book seller.

The Web services are outside the network perimeter are still within the sphere of business operations of the book seller. The concept of a network perimeter is still useful from a network engineering and maintenance perspective; from a business and operational perspective, the boundaries between inside and outside the organization are becoming more fluid (see Figure 1.1)

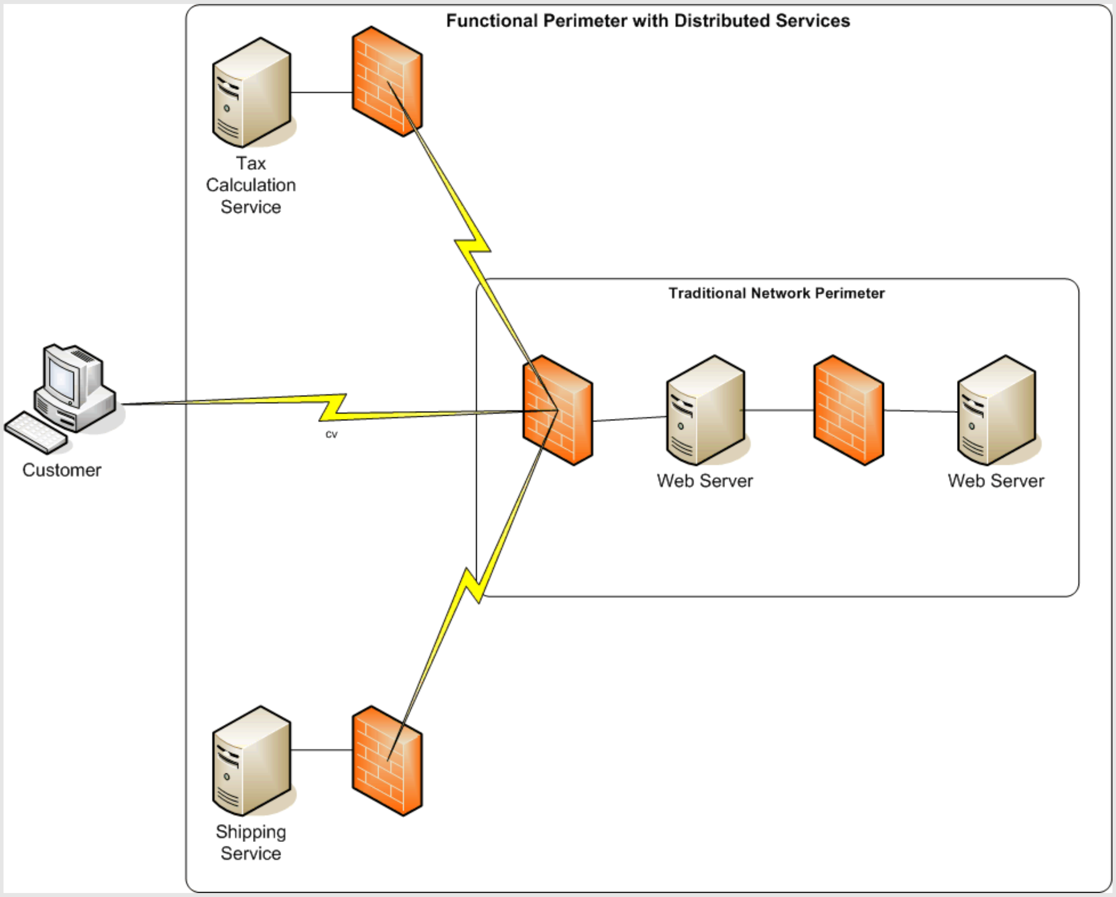
Functional Perimeter with Distributed Services
Tax Calculation Service
Traditional Network Perimeter
Customer
cv
Web Server
Web Server
Shipping Service

Figure 1.1: The concept of a network perimeter is not as clear cut as it was before the advent of Web services.

Protecting Data

In addition to protecting system infrastructures and core applications, organizations must protect the integrity and confidentiality of their data. Data lost as a result of systems failure or even malicious acts can be restored, albeit perhaps only partially, when sound backup and recovery practices are in place. Although small and midsized businesses and organizations may not have the level of failover recovery found in large enterprises, everyone should have effective backup and recovery procedures.

A more difficult problem to address is when a disgruntled employee or an outside attacker has tampered with data. In these cases, there may be no obvious, immediate signs of tampering. The tampering may not have a consistent pattern. In the worst case scenario, the only way to ensure the integrity of the data is to roll back to a point in time known to have reliable data and recreate all changes since that point.

A third type of data protection problem is extremely difficult to recover from—the loss of confidential data. Reports of stolen credit card and related identity information from major credit card processing services have made clear the level of this problem. In some cases, simply canceling credit cards and re-issuing new ones can solve the problem. In cases of identity theft, it can take individuals several months to resolve issues related to the theft.

Consequences of Identity Theft

With the right type of personal information, an identity thief can wreck havoc on someone's financial business. Some potential problems are:

- Tampering with existing accounts
- Unauthorized charges to credit cards
- Theft of funds from checking accounts
- Opening of credit cards using the stolen identity
- Incorrect entries on credit reports
- Applying for driver's licenses using the stolen identity
- Filing for bankruptcy using the stolen identity
- Making investments using the stolen identity

According to a 2003 survey by the United States Federal Trade Commission (FTC), consumers lost $5 billion and businesses $47.6 billion in out-of-pocket expenses due to identity theft. The vast majority of identity thefts have been the result of theft of information from offline sources, such as paper records and postal mail. Recently, though, sophisticated keylogging programs have been discovered that can collect password and logon information, disable the Windows firewall, and modify system files to prevent access to security vendors' sites so that victims cannot update their antivirus and other security software. Expect the proportion of identity thefts originating online to grow. For more information about identity theft, see the United State Federal Trade Commissions site on identity theft at http://www.consumer.gov/idtheft/.

📖 See the section "Regulatory Compliance" later in the chapter for more information about data confidentiality.

Losing confidential business data—such as sales lists, proposals, product designs, legal briefs, and strategy documents—can devastate a business. Imagine a small startup with a proprietary method for producing a low-cost, high-quality wireless device with applications in medicine, telecommunications, and public safety. Suppose an attacker compromises a server with information about the process and posts details on the Internet.

Protecting information assets, including hardware, software, and data, is a multifaceted problem. In the case of natural disasters, the best you can do is to implement plans that allow for rapid recovery when they do happen. In the case of malicious acts, you can utilize best practices in information security management to detect, isolate, and eliminate those threats.

Efficient Operations

The need for efficient operations has been around at least as long as free markets have existed. The advent of information technology (IT) has produced more tools with which to redesign and reengineer operations; it also brings with it the potential for adverse affects on efficiency. Consider a few examples:

- Email has streamlined communications within and across organizations; however, this tool has also brought large volumes of spam, phishing attacks, and increased storage requirements due to poor document management practices (for example, attaching a large file and sending it to dozens of recipients instead of emailing a link to the file).
- Internet browsers are becoming the new client desktop as well as providing access to stores of information on the Internet. It is also the stepping stone to time-wasting sites such as online casinos.
- Computers that have been compromised by malware may contain programs that launch Denial of Service (DoS) attacks. In these attacks, compromised computers flood Web servers with bogus network traffic in an attempt to overwhelm the Web site. In addition to shutting down the target of the attack, the compromised machines are wasting bandwidth and computing cycles on the compromised network.

Making the most efficient use of computing and networking resources requires a combination of technology—such as antivirus applications, firewalls, and content filtering—and policies about appropriate use of information assets, such as using business systems for business operations only.

📖 In the past few years, there has been heated debate within the business community about IT efficiency and competitiveness. The discussion here does not delve into those broader issues and instead examines efficiency from a security management perspective. For more information about the broader debate, a good starting point is Nicholas Carr's "Does IT Matter?" at http://www.nicholasgcarr.com/doesitmatter.html and John Soat's response to Carr in "Book Review: IT's Transformational Effect: The Real Point" at http://www.informationweek.com/story/showArticle.jhtml?articleID=51201618.

Non-Threatening Work Environment

Employers are responsible for ensuring a non-threatening work environment to employees. It should be no surprise that the pervasive reach of the Internet has touched this aspect of organizations along with so many others.

In a non-threatening work environment, employees and contractors are not subject to unwelcome harassment or exposed to offensive material. Today, that harassment can take the form of

- Offensive emails sent by employees to others in the organization
- The display of inappropriate material in a colleague's Web browser
- Offensive postings on an intranet discussion group

Employers cannot control the behavior of employees, but they can utilize a combination of policies and technology to define and enforce legitimate boundaries of discourse in an organization.

Protecting Against Loss of Controlled Information

In spite of the information overload experienced in today's business world, information is an increasingly valuable asset. From a security perspective, there are three types of controlled information that warrant particular attention:

- Intellectual property
- Proprietary data
- Private information

For some organizations, the most valuable assets are not their buildings, equipment, and other tangible assets but their intellectual property. Proprietary processing methods, deep knowledge of their customer's business needs, and trade secrets about designs of products are valuable targets for attackers and thieves.

Proprietary data includes information about business strategies, customer proposals, budget details, and operational reporting. Like intellectual property, this information would be especially useful to competitors. In some cases, proprietary data is eventually made public—for example, a public company may announce a major contract with a new customer; if the information were obtained prior to public disclosure, it could be used to influence illegal investment decisions.

Private information is data about customers, employees, and others who provide personal information to an organization. Loss of private information can damage the reputation of a business and, in some cases, lead to eventual business failure. CardSystems Solutions, a credit card transaction clearing house, lost the business of Visa and American Express shortly after a major security breach occurred resulting in the exposure of 40 million identities.

Although protecting all three types of controlled information is the responsibility of any business, the need to protect such private information is coming more under the direction of government regulation.

Regulatory Compliance

Regulation from multiple governments concerning individual privacy and the integrity of public companies is a fact many IT organizations must address. The growing public awareness for the loss of privacy in the information age has occurred at roughly the same time as several high-profile investor fraud cases, such as Enron and WorldCom. Not surprisingly, regulations about privacy and business integrity have emerged in response.

The first thing to understand about these regulations is that there are too many from too many sources to mistake the new regulatory environment as a passing fad. For example, consider some of the governments that have passed regulations that impact IT operations.

Privacy regulations include:

- State of California, United States passed State Bill 1386, a law directing companies and government agencies to inform California residents of any unauthorized disclosure of personal information.
- The United States passed the Health Insurance Portability and Accountability Act (HIPAA), which dictates how personal medical information is used and shared. It also establishes security standards for healthcare providers to ensure private data is adequately protected.
- The Gramm-Leach-Bliley Act includes privacy and security regulations that govern how banks collect private information, how consumers may opt-out of information sharing programs, and directives for ensuring unauthorized changes are not made to private information.
- The Australian Federal Privacy Act defines principals for the collection and use of personal information of Australian citizens by businesses and governments.
- The European Union (EU) Directive 95/46/EC defines regulations about how personal data is collected, stored, shared, and updated.
- Canada has passed the Personal Information Protection and Electronic Documents Act (PIPEDA), defining standards for protecting personal data.

Business integrity regulations include:

- The Sarbanes-Oxley Act, which is perhaps the most well-known government regulation, was issued in response to recent corporate and investment scandals. This regulation broadly covers the governance of public companies. Its impact on IT operations focuses primarily on ensuring the integrity of financial reports, ensuring internal procedures are appropriate to guarantee data integrity, and reporting material changes in a company's operations.
- Title 21, Code of Federal Regulations, Part 11 (21 CFR Part 11) was created by the United States Food and Drug Administration (FDA) to define proper controls on the use of electronic signatures and electronic documents in the pharmaceuticals industry.
- Basel II was created by the Bank for International Settlements, an international organization designed to promote cooperation in international banking, to ensure banks properly manage and report credit risks.

Compliance and Security

Although government regulations are varied in context, they share a common requirement—protecting data from unauthorized access and changes. Rather than try to create policies, procedures, and technical solutions to individual regulations, a common security framework that addresses access controls, identity management, and content filtering, combined with other information security tools and techniques can solve the problem.

📖 For more information about best practices in IT compliance, see the Information Systems Audit and Control Association Web site at http://www.isaca.org/.

Summary of Organizational Responsibilities

Businesses, governments, and other organizations that use IT share many common responsibilities. First, they must protect information assets, including the hardware, software, and network infrastructure that constitutes their IT infrastructures. Just as importantly, the information housed within that environment must be protected. Second, they must ensure efficient operations for the benefit of stakeholders. Just as finances and personnel must be managed effectively, so too do information assets. Third, employers are responsible for preserving a non-threatening environment for employees. Widespread use of Internet technologies introduces new venues for harassing activities and events. Fourth, organizations must ensure the integrity of controlled information, including private customer data as well as proprietary information. Finally, businesses and some government agencies must comply with specific regulations governing privacy and business integrity.

Sound security management practices are essential to meeting these obligations. Although no single security practice or tool will address all threats, the proper combination of them will. The emphasis of this guide is on a set of Internet-based threats that will now be addressed.

Threats Posed by Internet Content

There are many threats to information security on the Internet, including attacks that render servers unavailable for legitimate operations, attacks that steal information by "eavesdropping" on other's communications, and attacks that use the transmission of content as a mechanism for attacks. The most prevalent problems associated with Internet content are:

- Viruses, worms, Trojan horses, and other malware
- Spyware
- Phishing
- Spam
- Undesirable Web sites

Each of these presents distinct problems to the integrity of IT operations. Later chapters will delve into the details of these topics; the following sections provide a brief overview.

Viruses, Worms, Trojan Horses, and Other Malware

Malicious software is a well-known problem for which there are many solutions. Unfortunately, the problem is constantly evolving in response to defensive measures deployed by Internet users. One of the earliest forms of malicious software, the virus, is still around but has changed radically since the early days of PC adoption when viruses spread by copying themselves to floppy disks. In addition, new forms of malicious programs, including worms, Trojan horses, and blended threats endanger IT assets. The first step to understanding how to prevent damage from these malicious programs is to understand what they are and how they work.

Computer Viruses

Computer viruses are the best known type of malicious software and have been a problem since before the Internet's widespread adoption. Computer viruses are programming code that attach themselves to other programs, perform destructive tasks such as deleting files, and make copies of themselves. A variation on the traditional virus is the macro virus.

Macro viruses attach themselves to data files, such as word processing documents and emails, rather than executable programs. These viruses take advantage of embedded programming systems, such as Visual Basic Script (VBScript), which allow documents to execute custom code.

Traditional Virus Detection

Traditional viruses and macro viruses are relatively easy to detect. Once a virus is discovered, antivirus developers can identify unique patterns within the program code that identify the virus, much like a fingerprint can uniquely identify a person. This identifying pattern is known as a signature. Antivirus software consists of an antivirus engine, which analyzes content such as files on a disk of data transmitted over a network, and compares that content to signatures in the tool's virus library. Antivirus vendors are constantly updating their library of signatures and making them available for download.

Mutating Viruses

Not to be outdone by antivirus developers, virus writers developed a radically new technique for creating viruses that do not have distinct signatures. Known as mutating viruses, these malicious programs copy themselves and continue to perform malicious tasks, but unlike traditional viruses, they do not make identical copies. Instead, they introduce useless instructions in the code and rearrange the order of instructions in every copy. In this manner, there is no distinctive pattern, like a finger print, to use for identification.

For example, a traditional virus might employ a sequence of instructions, known as the payload, such as:

- Read data from register 1 into memory location A
- Set interrupt 21
- Write "Infected by XYZ" in COMMAND.COM at location B.
- …

A mutating virus will use a piece of code known as a mutation engine to add useless commands and rearrange the order of instructions not dependent on each other, creating something like the following:

- Write 1+1 to memory location B
- Read data from register 1 into memory location A
- Read data from register 1 into memory location B
- Set interrupt 21
- Write 0-0 to memory location C
- Write "Infected by XYZ" in COMMAND.COM at location B.
- …

The result is that the net effect of the virus is the same, but it appears to be a different program from the one identified by the virus signature for the first set of instructions. The emergence of mutating viruses forced antivirus developers to change strategies and move from identifying viruses by their structure to identifying viruses by their behavior.

Worms

Worms are similar to viruses in that they are self-replicating, malicious programs. Unlike viruses, worms are fully functional programs; they do not need to attach themselves to an executable or document file to spread. Worms often exploit mail and file transfer services available to compromised machines to propagate.

- The Melissa worm demonstrated the effectiveness of mass emailing of malware in 1999 when it spread around the world in 2 days. The worm emailed itself to the top 50 or 100 (depending on the version) names in the infected user's Outlook Address book.
- The Sasser worm emerged in April 2004 and exploited open ports in firewalls to spread. Sasser used FTP to download malicious payload, then replicated using the same protocol.
- SQL Slammer exploited a vulnerability in the Microsoft database, SQL Server, and reached 75,000 victims in 10 minutes in January 2003. SQL Slammer is a simple worm that generates random Internet Protocol (IP) addresses and copies itself to those addresses. If the host with that address happens to be running an unpatched version of SQL Server, it becomes infected and begins to spread the infection.

As worms do not depend on other programs to act as carriers to spread, they can replicate rapidly. Viruses typically activate when the infected executable is run or infected document is open; worms are not slowed by waiting for a user to act on a program or file.

> 🕮 For more information about Melissa, Sasser, SQL Slammer, and other worms and viruses, see the McAfee Virus Information Library at http://vil.mcafeesecurity.com/vil/.

Trojan Horses

Trojan horses are malicious programs that appear useful and benign. Unlike viruses and worms, Trojan horses do not replicate themselves. Instead, a programmer either includes a piece of malicious code in an otherwise useful program (for example, a disk utility) or disguises the program as something completely different, such as an electronic greeting card. In either case, once the file is downloaded and executed, the malicious code can execute. Trojan horses are used for a variety of tasks, including:

- Deleting files
- Corrupting data
- Using computing resources of the compromised machine, for example, to conduct spam or phishing mass emailings or to launch DoS attacks
- Capturing identity information, such as usernames and passwords, with keylogging programs
- Downloading adware

Viruses, worms, and Trojan horses are some of the oldest and most common forms of malware, but there are others as well.

Additional Forms of Malware

Malicious code, or malware, has evolved into multiple forms. Viruses and worms are well known because they spread so rapidly, but other forms of malware can be just as—and in some cases more—dangerous than either. Other forms of malware include:

- Keyloggers, which are programs that record a user's keystrokes and transmits them to a server on which usernames, passwords, credit card numbers, and other useful information can be captured.
- URL Injection programs change a user's URLs to make it appear that a user is browsing to a site, such as Amazon.com, from an affiliate site.
- Backdoor programs allow attackers to gain control of a computer without the knowledge or authorization of its user. These programs are sometimes used to launch DoS attacks and mass mailings of spam and phishing lures. Computers compromised by backdoors are often called zombies.
- Rootkits are the most dangerous form of malware. These are sets of programs used by attackers to maintain control of compromised computers and erase traces of their activities. As rootkits can modify system files and disguise changes, the only way to ensure a rootkit is removed is to format disk drives and reinstall the OS, applications, and data.
- Blended threats are programs that package several types of malware, often including worms, keyloggers, and even email, file transfer, and other communication programs.

Another form of malware that has grown into a serious threat to both corporate and home computer users is spyware.

Spyware

Spyware is a form of malicious software that captures information about users or otherwise takes control of system resources without the user's knowledge or consent. Spyware emerged in the late 1990s and had reached epidemic levels by 2004. In that year, a survey by America Online and National Cyber-Security Alliance found that 80 percent of the computers surveyed had some form of spyware on them, and there were an average of 93 pieces of spyware on each machine. The vast majority of users, 89 percent, did not know these programs were on their computers.

> 📖 For details on the AOL/NCSA spyware survey, see http://www.staysafeonline.info/news/safety_study_v04.pdf.

The most dangerous effects of spyware include:

- Loss of privacy and identity theft
- Decreased system performance
- System crashes as a result of poorly designed and written software
- Disabled security software, such as antivirus and firewalls, which leaves systems vulnerable to other malware infections

Less destructive but still problematic effects of spyware include:

- Displaying unwanted pop-up advertisements
- Changing search engine results
- Changing host files and other networking files causing users to unintentionally navigate to spyware-promoted sites

Spyware is spreads as Trojan horses, such as in Internet toolbar add-ons, and through the ability to manipulate browser vulnerabilities, especially in IE.

Phishing

Phishing is a relatively new method for age-old con schemes. The purpose of phishing is to trick users into disclosing valuable information such as credit card numbers, Social Security numbers, driver license numbers, and other personal information. In the most audacious scams, phishers attempt to convince victims to send money to a "charity" or "investment opportunity."

A phishing scam begins with a lure, such as a request to update account information or verify account numbers. Financial institutions are commonly used in these phishing lures. Recent scams have targeted eBay, PayPal, Citizens Bank, Ameritrade, Bank of America, and Comcast.

> 📖 For examples of phishing lures, see the Anti-Phishing Working Group's Phishing Archive Web site at http://www.antiphishing.org/phishing_archive.html.

Lures typically contain links to bogus sites where users are prompted for identifying information. Phishers will often use HTML and scripts from legitimate sites to make their bogus versions appear legitimate. Ways to identify a phishing scam include:

- Misspelled URLs, for example www.bankofamericas.com instead of www.bankofamerica.com
- Ungrammatical or unusual greetings, such as "Dear PayPal" or "Dear Value Customer"
- Random strings of characters in the message—these are used to trick spam and phishing filters that look for specific patterns of text in messages

Phishing lures are just one type spam that has created many problems for email administrators and users.

Spam

Spam is unsolicited, unwanted email. It's an obvious problem for users with inboxes that are cluttered with junk email, but that is just the tip of the iceberg. Spam creates several problems for email and network administrators:

- The need for additional storage space to store unwanted, unsolicited emails
- The threat of malware or phishing scams being carried by spam message
- Taxed bandwidth, especially when delivering messages to client's over slow network connections
- Lost time and productivity cleaning up spam

As with other threats, systems administrators have responded with spam management practices, such as quarantining suspected spam and blocking emails from known spamming sources. Although these methods reduce the eventual number of spam messages that make their way to user inboxes, these practices require additional technology that, in turn, requires maintenance and change control processes. Spam is not going away, so the best approach to managing it is to deploy a spam management system that accurately identifies spam while minimizing the demands on systems and network administrators.

Undesirable Web Sites

Businesses and other organizations commonly have policies about the proper use of IT resources, including Internet browsing. Outside of highly secure government and business networks, few employers are likely to be concerned with an employee occasionally checking the latest news or stock quote. Problems arise when employees use company resources for offensive or time-wasting activities.

One of the responsibilities of organizations in general is to provide a non-threatening work environment. This requirement includes ensuring that offensive material is not circulated or stored within the organization's network, email systems are not used to transmit offensive material, and employees do not download such material. Creating a threatening environment is only one of the problems posed by employee use of the Web.

Time-wasting Web sites are easy to find. At least hundreds of gambling sites, online games, political blogs, personal ad sites, music and video sites, and online shopping are readily available on the Web. In addition to reducing productivity, visiting such sites can expose the user's system to spyware, adware, Trojan horses, and other types of malware. File sharing services are a commonly used means of distributing malware. The major threats from Internet content—malware, spyware, phishing, spam, and the use of undesirable Web sites—must be addressed using a combination of technology and user training.

Countermeasures to Threats

The majority of this chapter has focused on high-level goals for managing information resources and the threats to those resources. The topic can become discouraging when one understands how many different ways there are to compromise systems, commit fraud, and steal personal and proprietary information. Fortunately, for each threat, there is a combination of technologies and procedures (including user education) that can significantly reduce these threats. The key technologies are:

- Content filtering
- URL filtering
- Antivirus software
- Anti-spyware
- Spam management

Much of this guide focuses on these technologies and how to apply them most effectively.

Content Filtering

Content filtering is a process in which network traffic is scanned for patterns that indicate dangerous or offensive content. Content targeted by these scans are blocked from transmission. Content filtering is used for email, Web browsing (HTTP), instant messaging, and chat and other text-based traffic.

Content filters use libraries of words and phrases that are typically found in target content. For example, phrases such as “live dealers,” “blackjack,” “payouts,” and “poker rooms” are indicative of an online casino. Similarly, organizations can specify terminology used in their business to identify proprietary information and prevent it from being transmitted outside the organization.

URL Filtering

URL filtering is similar to content filtering in that content is blocked; however, rather than focusing on a particular piece of content, URL filtering blocks all transmission to or from specific sites. This technique is especially useful for blocking established sites that are not relevant to business operations. For example, employers can prevent employees from checking personal email by blocking mail.yahoo.com, www.hotmail.com, and similar sites.

URL filtering software uses *white lists* and *black lists* to identify sites that have content allowed within an organization and those which do not, respectively. With rapid change in Web site registrations, it is difficult if not impossible to maintain a compressive list of disallowed sites. However, even with that limitation, URL filtering in combination with other technologies can help reduce the threats of malicious or inappropriate material entering or leaving a network.

Antivirus Software

Antivirus software is widely used on desktops; it can also be deployed at the enterprise level on email servers or other servers to scan content as it enters or leaves an organization's intranet. As noted earlier, antivirus programs use both static pattern-recognition techniques to identify known viruses and behavioral techniques to analyze the way a program operates to determine whether it is a virus.

Anti-Spyware

Anti-spyware systems operate in two ways—by filtering and blocking spyware before it can be installed or by detecting it and removing it after it has been installed. Like antivirus programs, anti-spyware systems detects tell-tale signs of spyware, such as tracking cookies used in Internet browsers, entries in Windows registries, or known spyware programs found on a system. It can also operate as a content filtering system, scanning incoming network traffic looking for similar indicators that a remote site is trying to install spyware on a local machine.

Spam Management

In some ways, managing spam should be easy; after all these are just email messages. They are not as complex as a mutating virus or a blended threat. It is a challenge, though, because distinguishing spam from legitimate email is not straightforward for several reasons. First, spammers know that businesses and Internet service providers (ISPs) use spam management tools to block their mass emailings. They carefully craft spam messages to minimize the use of tell-tale characteristics:

- Hide recipient's email address in the BCC: section of the header
- Improper or empty TO: address
- Large number of recipients in the TO:, CC:, or BCC: fields
- X-mailer field contains names of known spamming software
- Unusual use of HTML, such as an excessive number of comments to hide spam text
- Offer phrases such as "Click here now," "free," "earn money," and "limited time offer"

In addition, spam management software should not block legitimate email. Just because an email has a large number of recipients or a few questionable phrases does not necessarily mean it is spam. No anti-spam filter will ever be 100 percent accurate, but spam management vendors try to minimize the number of false positive hits (that is identifying a legitimate email as spam) while also minimizing the number of false negatives (that is identifying a spam message as legitimate email).

A combination of countermeasures is essential to ensuring the content flow in and out of an organization is properly managed to minimize threats to the organization, its employees, and its information assets.

Countermeasure Implementations

Countermeasures are implemented in three ways:

- Software applications
- Services
- Appliances

Software applications, as classified here, are countermeasures that execute within an intranet and perform antivirus, anti-spam, anti-phishing, and other content filtering operations. As with other software applications, they are installed and maintained by systems administrators.

Services are software applications that provide the same type of services but do so from an Internet accessible server outside an organization's intranet. These services may use similar software to that which is deployed within an intranet, but it is maintained and updated by the software vendor or a third party.

The third way to implement countermeasures is with an appliance. An appliance is a network device that is easily configured and performs countermeasure tasks with minimal maintenance or system administration. This ease of deployment, use, and administration is a major benefit of this method of delivering counter measures.

📖 More details of the advantages and disadvantages of these countermeasure implementations will be discussed in future chapters.

Summary

Businesses and organizations depend on the Internet to function, yet this critical piece of infrastructure comes with significant threats. Some of the most pressing for today's IT professionals are viruses, worms, and other malware; phishing scams; spam; and the inappropriate use of IT resources, especially Internet access. The remaining chapters will examine technologies and practices available today to help mitigate these threats and allow organizations to focus on the core business.

Content Central

Content Central is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, learning about new development tools for Windows and Linux, or deploying new enterprise software solutions, Content Central offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

Download Additional eBooks!

If you found this eBook to be informative, then please visit Content Central and download other eBooks on this topic. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to other great IT eBooks and video guides. Please visit: http://www.realtimepublishers.com/contentcentral/.