Realtime
publishers
"Leading the Conversation"

The Shortcut Guide™ To

Protecting Business Internet Usage

sponsored by

SurfControl®

Dan Sullivan

Introduction to Realtimepublishers

by Don Jones, Series Editor

For several years, now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 1: Preserving Business Integrity

Organizations depend upon reliable and secure Internet access to conduct business, yet of all the venues for conducting commerce and other operations, the Internet poses some of the greatest challenges:

- How can businesses protect private and confidential information?
- How can one be sure data is not tampered with in transmission?
- What regulations are applicable to Internet content?
- Is the current state of network and related infrastructure secure?

These are just some of the questions facing organizations that depend upon the Internet. This guide is designed to address some of the most pressing questions facing executives and IT managers with regard to protecting the use of Internet access and Internet content for business, government, and other organizations.

This first chapter addresses the problem of preserving business integrity, beginning with the business case for expending time and resources to ensure the integrity of Internet access and content. Although compliance is a term that is too often used to grab attention and headlines, it is a topic central to the issue of business integrity in general and is highly relevant to business use of the Internet. Business integrity has both an external and internal dimension. In the latter case, organizations must control the workplace environment and address the human resource issues that can arise with widespread use of Internet technologies. Of course, the Internet has not changed the nature of workplace issues, but it has changed methods of challenging as well as controlling the work environment. Finally, a brief discussion of Internet-based threats and corresponding countermeasures concludes this chapter.

Business Case for Preserving the Integrity of Content Flows

A common exhortation heard during the early days of business adoption of the Internet was “the Internet changes everything.” After the dot com bust, we all have plenty of counterexamples to that naivety. (A business that sells pet food at a loss over the Internet does not succeed by launching a major ad campaign and selling more products.) Clearly, many business basics from the pre-Internet period remain the same today.

Businesses and organizations spend a great deal of time and effort ensuring they abide by laws and regulations, protect their assets, and attend to the needs of employees—all in addition to providing the products and services at the core of their business. Legitimate companies would not fail to lock the doors at night, properly secure dangerous equipment and materials, or file tax returns. These are all part of running a business. Yet some highly publicized cases have demonstrated a profound lack of understanding of the measures required to protect business Internet access. The Internet has not changed everything, but there have been enough changes to warrant an examination of changing business practices.

The Changing Landscape of Business Practices

The widespread use of the Internet in business has created opportunities as well as responsibilities.

The Way We Were …

Consider an example in brick-and-mortar retail commerce. A customer makes a purchase at a store and pays with a credit card. The store keeps the merchant's copy of the receipt and stores it in a locked cash register until the clerk closes out the drawer. After that, the receipt is moved to a back office where transactions are reconciled. The cash and receipts are secured according to sound business practice.

The objective here is not to make work for the accounting office (chances are they have enough) and this "overhead" work has no direct benefit to the customer; it certainly does not have a direct benefit to the bottom line, yet countless businesses around the world carry out these and more elaborate practices every day. Why? To protect the integrity of the business.

Imagine a business without these or similar practices; they would face several potential problems:

- Customer receipts might be lost or stolen
- The task of reconciling accounts could become difficult
- Customer disputes could not be resolved fairly because key documentation, such as credit card receipts, is missing
- Customers could become victims of identity theft or other fraud because personal financial information is mishandled

The end result would be a short-lived business

…Is Largely Who We Are

Although some of the policies and practices of successful business operations are so commonplace they seem obvious, others are not. The Internet, for example, has introduced radically different ways of doing business. Customers can order products with little more than a browser, a PC, a modem, and a dial-up connection. Suppliers can monitor inventory levels of their customers and ship products without so much as a phone call from the customer. Clearly basic business transactions, from shipping packages to ordering supplies to providing customer service, are done differently now than they were 20 or even 10 years ago.

One of the challenges facing businesses that leverage the advantages of the Internet is developing sound business practices that protect the integrity of the business. We have well-defined and well-known best practices for traditional commerce; best practices for e-commerce and other Internet-centric operations are less popularly known. Fortunately though, best practices do exist and there are measures businesses and organizations can take to protect the integrity of their operations.

Best Practice Areas for Business Internet Access

Not surprisingly, the best practice areas for business Internet access largely overlap with other business areas. Some of the most important aspects of business integrity with respect to the Internet focus around:

- Maintaining accurate, complete, and timely information about the state of the business
- Protecting private information and confidential and proprietary company information
- Preserving appropriate working conditions for all employees
- Ensuring employee productivity

Although these goals overlap, the mechanisms by which businesses and other organizations reach these goals are different. The Internet has forced organizations to expand the policies and procedures that have protected business integrity to include new technologies.

Organizational Policies for Internet Access and Content Control

The purpose of policies with regard to Internet access and content control is to protect the organization, its employees, and its resources. Polices can help to address issues as wide ranging as data theft protection, intellectual property protection, and preventing a hostile workplace. (The last topic will be addressed in the next section). Unfortunately, the effective adoption of protective policies and procedures is lagging behind the technological adoption of the Internet.

The lack of policies, or their poor implementation, is reaching the general press. Large-scale data thefts are making headlines and with good reason—consumers are fearful of the growing problem of identity theft. Consider some recent, high-profile thefts:

- CardSystem Solutions—Credit card information about 40 million customers stolen
- Choicepoint—145,000 names, addresses, and Social Security numbers stolen
- Lexis-Nexus—300,000 have personal information stolen
- Citigroup—UPS loses a box with backup tapes containing personal information about 3.9 million people
- Department of Veterans Affairs—Personal data about 26.5 million veterans compromised

The theft of credit card data and other personal information by attackers who break into banks and financial institutions can readily grab headlines. Another problem that is less likely to garner the big headlines is the loss of intellectual property.

Intellectual property covers a wide range of practices, techniques, and proprietary processes that give businesses a competitive advantage. Microsoft suffered intellectual property loss in 2004 when 30,000 files containing source code from Windows Service Pack 1 (SP1) were leaked to the public.

For more information about the Microsoft intellectual property loss, see “Windows Source Leak Traces Back to Mainsoft” at http://www.osnews.com/story.php?news_id=6005.

Protecting information in an environment as open and as connected as the Internet requires comprehensive planning and multilayered defenses. No single technique—such as encryption, access controls, or content filtering—will solve the entire problem, but these and other techniques are essential elements of the overall solution. Although these techniques address how to enforce security, policies define what the security practices should be.

Clearly, protecting business integrity is not a new problem with the Internet; the changes in communication methods and business infrastructure have simply expanded the scope of applicability of business responsibilities, such as compliance and the preservation of non-hostile workplaces.

Compliance and Internet Security

As noted earlier, the term *compliance* is getting a great deal of press these days. This recognition is understandable; governments from the state to transnational levels are defining regulations in response to actual and potential lapses in the protection of financial and personal information. Just the mention of businesses such as Enron, WorldCom, Tyco, and Arthur Anderson bring to mind the consequences of poor corporate governance and the resulting lack of information integrity essential to business. Similarly, widely publicized security breaches at credit card processors and major financial institutions make clear the need for additional measures to protect personal financial information. These incidents are examples of the types of failures to protect the integrity and confidentiality of information that regulations are designed to prevent. Regulations, at least with regard to protecting information, can be broadly classified into integrity preservation and confidentiality protection.

Information Integrity Regulations

The goal of protecting information integrity is to ensure that the trust required for a business to function is not threatened by manipulations of information. For example, when a publicly traded company publishes income statements, cash flow statements, and balance sheets in their quarterly and annual reports, analysts, investors, and government officials will assume the reports are accurate reflections of the state of the business and act accordingly. One of the benefits of this transparency of operations is that it reduces investment risks.

Obviously, investors are less likely to move capital into countries that have limited transparency in business operations because “off book” deals and other hidden aspects of a business can undermine the value of whatever information is provided. In the case of the Enron debacle, investors where unaware of the labyrinth of deals with shell companies and the movement of debt and profits between corporate entities that hid the true state of the company’s finances. One of the responses in the United States to Enron’s collapse, and similar corporate deceptions, was the passage of the Sarbanes-Oxley Act.

The Sarbanes-Oxley Act, commonly known as SOX, has several provisions:

- Definition requirements for board membership
- Require the board to establish audit and quality control standards
- Prohibit activities on the part of auditors, such as consulting to audit clients
- Corporate responsibility for corporate reports
- Disclosure of periodic reports
- Management assessment of internal controls, commonly referred to as Section 404

The ones most relevant to IT concern internal controls. IT plays a key role in preserving the integrity of financial data, and publicly traded companies are now required, under SOX, to document IT control mechanisms. In addition to storing information about the finances, sales prospects, and related operational information, IT systems must be auditable, must use access controls to prevent unauthorized changes to information, and must change as necessary to support emerging reporting and compliance requirements.

📖 For more information about SOX, see the American Institute of Certified Public Account's summary at http://www.aicpa.org/info/sarbanes_oxley_summary.htm. For the full text of the act, see http://fl1.findlaw.com/news.findlaw.com/cnn/docs/gwbush/sarbanesoxley072302.pdf.

In addition to information integrity, regulations have addressed the need to preserve the privacy of personal information.

Privacy Regulations

Unlike the domain of integrity regulations in which a small number of comprehensive regulations exist, the area of privacy regulation is made up of large number of regulations. Some of the most well known are:

- Health Insurance Portability and Accounting Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- California SB 1386
- European Union (EU) Privacy Directives
- Other national privacy regulations

Together, these regulations span business area (such as healthcare and financial services) as well as geographic boundaries.

HIPAA

HIPAA covers several areas related to healthcare in the United States; one of the most important is the definition of protected health information (PHI) and rules governing the use and dissemination of that information. The act describes general principals for the use and disclosure of PHI as they apply to health plans, healthcare information clearinghouses, and healthcare providers. The main points of the regulation are defined in the Privacy Rule and the Administrative Simplification Rules.

📖 For more information about HIPAA, see http://www.hhs.gov/ocr/hipaa/. For details of the privacy and related rules, see http://www.hhs.gov/ocr/privacysummary.pdf.

GLBA

GLBA, also known as the Financial Services Modernization Act, redefined the competitive landscape of financial services, securities firms, and insurance companies. The act contains new regulations regarding the protection of personal financial information. The act specifies three rules:

- The Financial Privacy Rule defines the privacy agreement between an institution and its customers and governs, among other things, how the customers' information is shared with third-parties not affiliated with the institution.
- The Safeguards Rule requires institutions to define, implement, and test a plan to protect customer information.
- The Pretexting Rule requires financial institutions to implement measures to prevent customers from becoming victims of information theft through social engineering methods. These include impersonating a customer when calling the institution's customer support center and using spoofed emails to appear to be from a customer.

📖 For more information about GLBA's privacy protections, see http://www.ftc.gov/privacy/glbact/glbsub1.htm. For links to related topics and resources, see http://www.keytlaw.com/Links/glbact.htm.

In addition to federal regulations, states have also moved to address privacy concerns of their residents.

California SB 1386

California passed SB 1386 in 2003 in an attempt to protect it citizens from identity theft. The act requires organizations conducting business with California residents to notify those residents in the event of a security breach that could have disclosed their personally identifying information.

📖 The text of California SB 1386 is available at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

The United States has taken a decentralized approach to privacy protection using federal legislation to target particular types of information, such as health and financial information, while states fill in with broader legislation, like SB 1386, when they deem it appropriate. Many other countries have taken a more centralized approach.

EU Privacy Directives

The EU has specified two major directives to protect the privacy of its citizens as understood within the context of the European Convention on Human Rights. The first directive, EU 95/46/EC, is a set of requirements designed to define the actions organizations need to take when collecting and storing personal information. The regulation states that personal information can be collected and stored only with consent, only used for stated purposes, must be kept accurate and up to date, and may not be transferred to non-EU countries that do not provide equivalent privacy protections.

✎ The non-transfer requirement was problematic for European-US trade because the Unite States does not have comprehensive and national privacy regulations. A compromise, known as Safe Harbor, was reached in 2000 between the European Commission and the U.S. Department of Commerce. For more information about this topic, see http://www.export.gov/safeHarbor/index.html.

The second regulation, EU Directive 2002/58/EC extends privacy protections by requiring telecommunications providers to safeguard transmissions, prohibiting surveillance, and limit the amount of customer information collected and the length of time it is kept. It also addresses spam by allowing direct email marketing with consent of the recipient.

📖 For more information about the EU privacy protections, see http://ec.europa.eu/justice_home/fsj/privacy/.

National privacy protections similar to those of the EU have also been established in Canada, through the Personal Information Protection and Electronic Documents Act (PIPEDA), and Australia, through the Australian Federal Privacy Act.

Ensuring compliance with a multitude of regulations can challenge even the most well-run organizations. However, a common best practice for maintaining compliance is defining and enforcing relevant policies.

Compliance, both with regards to information integrity and privacy protections, often addresses how businesses and other organizations work with customers and constituents. A parallel set of issues arise within these same organizations when dealing with human resource and workplace issues.

Human Resources and Workplace Issues

The responsibility of employers to maintain a productive and non-hostile work environment is becoming more clearly defined. Productivity has always been a concern of management, but the advent of globalization, downsizing, and outsourcing, along with other factors in the business environment, keeps productivity a focal point for executives and managers. The past several decades have witnessed a growing intolerance for hostile work environments as reflected in case law decisions on the topic. When addressing the human resource and workplace issues, the three key objectives are

- Preventing a hostile work environment
- Maintaining productivity
- Controlling IT resources

The three objectives are often addressed independently but, in fact, tools designed to support one of these objectives can often support the others as well.

Preventing Hostile Work Environments

The issue of hostile work environments is difficult to address for several reasons, not the least of which is defining what the term means. At the risk of including events, artifacts, and opinions that do not fall into this category, and similarly excluding some that do, we will assume a hostile workplace is a work environment in which speech, acts, and displays by employees are severe and harassing enough so that reasonable employees feel harassed. As one law school professor points out, there have been many interpretations of hostile work environments and have included:

- Bigoted remarks about political candidates
- Denunciations of a particular religion
- Nudity in classical art
- Broadcast of prayers over a public address system

Clearly, there will be some cases in which reasonable individuals will agree that an act creates a hostile work environment and others that do not. There is also a broad grey area. The inability to determine a precise definition can have a chilling effect on speech and displays in a work environment and some organizations will err on the side of caution rather than risk creating a hostile work environment.

> 🕮 For more information about the difficulty of defining what constitutes a hostile work environment, see Professor Eugene Volokh's "What Speech Does 'Hostile Work Environment' Harassment Law Restrict?" at http://www.law.ucla.edu/volokh/harassg.htm.

With the widespread adoption of email and Internet access, the challenge of controlling harassing behavior has taken on a technical dimension. In the past, harassment may have occurred through speech or the display of an offensive poster. Today, email can transmit offensive material to large numbers of recipients with little effort. In one case, *Smyth v. The Pillsbury Company,* an employee was dismissed for making violent threats against other employees in an email. In another case, *Bourke vs. Nissan Motor Corporation*, employees were dismissed after their employer had discovered personal emails, including crude sexual humor, were transmitted using the company's email system.

Employees, contractors, and others with access to high-speed Internet connections at work may find it tempting to download images, videos, and audio files while at work. In addition to wasting network resources for non-work related activities, the material could be patently offensive and therefore have no place in the work environment. Keeping offensive content out of an organization is a priority for any employer concerned with hostile workplace issues.

Clearly, employers face a difficult balancing act. On one hand, email and open Internet access can provide for increased productivity and accelerate the pace of business operations. On the other hand, the same tools can contribute to offensive and demoralizing work environments. Businesses, government agencies, and other organizations have a responsibility to control the content that comes into their networked environment.

Content filtering technologies are mature enough to provide high levels of accurate identification of offensive material while allowing non-offensive and work-appropriate content to pass without interruption. These tools are also effective countermeasures to time-wasting and productivity draining activities that involve the Internet.

Maintaining Productivity

The Internet, and the World Wide Web in particular, is a double-edged sword with regards to productivity. The ability to execute core business operations more effectively with the improved communication, collaboration, and information sharing is well demonstrated. However, the lure of the Web for non-work related activities is also clear. According to a Salary.com/AOL poll of 10,000 people, 44.7 percent cited Web surfing as their number-one time-wasting activity at work.

EWeek reports that 24 percent of respondents to a 2006 poll admitted to watching or listening to streaming media at least once a week; 17 percent used IM in the same time period, and 18 percent downloaded non-work related images, music files, and video clips.

> 🕮 Statistics are from "Wasted Time at Work Costing Companies Billions" http://www.salary.com/careers/layoutscripts/crel_display.asp?tab=cre&cat=nocat&ser=Ser374&part=Par555 and "As Crucial as Coffee: Web Surfing at Work" http://www.eweek.com/article2/0,1759,1963997,00.asp?kc=EWRSS03119TX1K0000594.

As with preventing a hostile work environment, blocking external content that is unrelated to work is becoming another administrative task, such as backing up servers and reviewing application logs. Content filtering software available today can use detailed databases of sites categorized into groups such as shopping, gambling, adult, hate speech, and other areas. The ability to control the content that enters a network is also a crucial element to controlling IT resources.

Controlling IT Resources

In addition to the legitimate traffic and data stored on organization's servers, there is plenty of unwanted material. Spam uses network bandwidth and server storage. Image files, videos, and music files consume large amounts of disk storage. Routers, servers, and other computing resources waste cycles processing unwanted content. Backups take longer to run and use more media than necessary because of the difficulty separating business data from digital junk. Unfortunately, these are the least-threatening problems of unwanted content. Unwanted content can include unwanted programs such as worms, viruses, Trojan Horses, spyware, keyloggers, video frame grabbers, and rootkits.

📖 Chapter 2 includes a more thorough discussion of these and related threats.

Protecting employees from offensive and harassing material in the workplace and maintaining the productivity of staff and the appropriate use of IT resources are clearly two distinct management concerns. The measures available to management to realize these objectives, such as establishing policies and implementing content filtering, overlap in their effectiveness in addressing both problems.

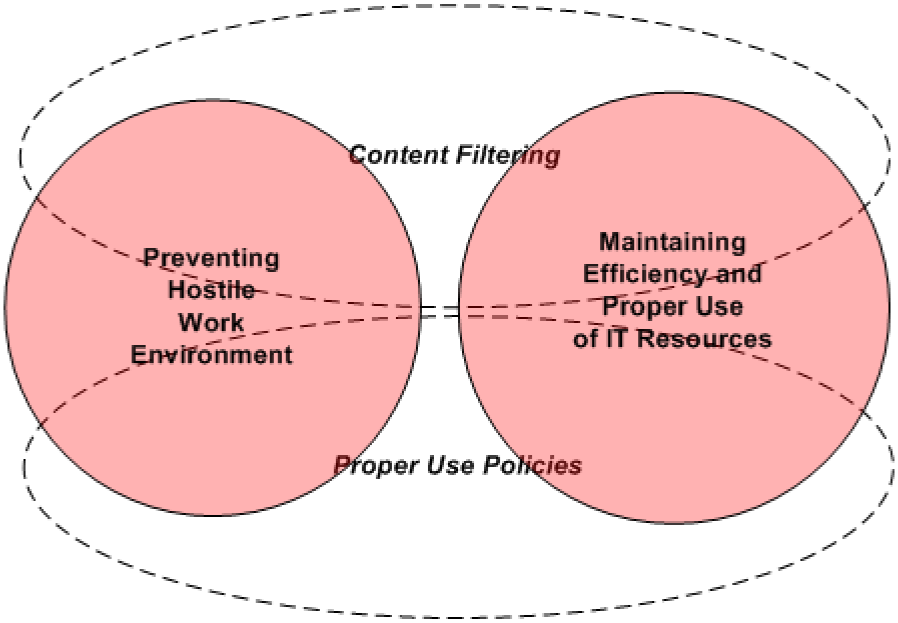
Content Filtering
Preventing Hostile Work Environment
Maintaining Efficiency and Proper Use of IT Resources
Proper Use Policies

Figure 1.1: Technologies for protecting Internet access and content flows often serve multiple purposes.

Protecting Business Internet Access: Fundamentals

Ensuring reliable and secure Internet services is a multifaceted challenge. To fully appreciate the breadth and depth of the task, it helps to understand three fundamental aspects of Internet access protection:

- Internet-based threats
- Structure and function of countermeasures
- Management issues

These aspects comprise the pillars upon which a comprehensive Internet access protection strategy is built.

Internet-Based Threats

Regardless of how you personally feel about hackers, scam artists, and Internet criminals, you must admit that they are creative. In the relatively short period of time since the widespread adoption of the Internet, there has been the development of a variety of malicious software and schemes to con the unsuspecting. Protecting against these threats is essential to preserving the integrity of Internet access; three of the most prevalent threats are:

- Malicious software, also known as malware
- Spyware
- Phishing scams

As the following sections will explore, there are effective countermeasures to these threats. Before we discuss them, let's first examine the characteristics of each of these threats.

Malware

Malware are programs designed to damage, disrupt, and compromise computers. Some of the best-known types of malware are:

- Viruses—Malicious programs that depend on another application or system to propagate
- Worms—Similar to viruses in that they carry a malicious payload but they do not require other programs to propagate
- Trojan Horses—Programs that purport to do one thing, such as synchronize your computer clock with time servers on the Internet, but also perform malicious actions such as stealing personal information
- Key loggers—Programs that record keystrokes and transmit them to a third party; these programs can be used to capture usernames and passwords
- Video Grabbers—Programs that make copies of video memory and transmit the contents to a third party
- Rootkits—Especially problematic forms of malware because they not only infect a device but also effectively hide their presence and the presence of other malware

First-generation malware was primarily viruses transmitted by infected diskettes, but the Internet opened a whole new set of methods for transmitting viruses, worms, and other malware. Email was an easy and obvious target for many virus writers but malware writers could target any program that uses the network. For example, the SQL Slammer worm that shut down large segments of the Internet in January 2003.

For a detailed description of the spread of SQL Slammer, see Paul Boutin's "Slammed!: An Inside View of the Worm that Crashed the Internet in 15 Minutes" at http://www.wired.com/wired/archive/11.07/slammer.html.

To add to the challenges facing network managers and security professionals, malware developers continue to improve the stealth characteristics of malware as well as the functionality of the payload. Antivirus writers initially detected viruses and related threats by looking for patterns of bits that were found only in those programs but not in legitimate applications. Virus writers began to encrypt viruses to avoid detection, but that ploy was easily countered by antivirus researchers and developers.

A fundamental shift in virus detection had to occur when virus writers started to use techniques to randomly change the pattern of bits in a program without changing the programs behaviors. (This can be done by introducing steps with no effect on calculations, such as adding 0 to a number or changing the order of execution of steps that do not depend on each other). Once again, antivirus researchers were able to counter these new threats with a new type of detection mechanism that examined the behavior or programs instead of their bit patterns. In addition to trying to hide their malicious code, malware writers improved the destructive and disruptive capacity of their threats.

Blended threats, for example, are malware programs that combine multiple threats. A single program might contain a Trojan Horse for carrying and transmitting the payload which in turn includes keyloggers, video frame grabbers, and communications programs for receiving commands from a central controller using a chat room or IRC channel.

Malware and other threats are discussed more thoroughly in Chapter 2.

Spyware

Spyware is a program that monitors a user's actions and/or collects information about users for third parties. Many consider spyware a form of malware like viruses and worms. From a technical perspective, spyware can be considered a form of malware because it uses similar techniques. From a deployment perspective, there are differences.

Some spyware developers prefer to call their products adware. The distinction is that adware allows a third party to collect information about a user and, based on their interests, target Internet ads appropriate to them. Adware may be incorporated in another application, such as a browser toolbar. In fairness to adware developers, some will note in their end user agreements that they collect information. This is a case of buyer beware; downloading a free application from the Internet that sounds too good to be true probably has a catch (spyware). Another threat to the unsuspecting Internet user is phishing.

Phishing

Phishing is a form of social engineering that attempts to get someone to reveal personal information—such as Social Security numbers, account numbers, or passwords—using false pretenses. Phishing is conducted with a combination of emails to lure the victim and bogus Web sites to collect information.

Early phishing scams often used the names of major companies such as banks and online retailers and sent messages about the need to verify information or warnings about unauthorized attempts to access the victim's online account. Some of the companies who were popular targets include Citigroup, PayPal, and eBay as well as numerous financial institutions.

As the companies responded with warnings to customers and customers themselves became more suspicious of messages from these companies, phishers modified their tactics. Phishing campaigns become more focused, targeting smaller numbers of potential victims and using smaller companies in their lures in a process that has come to be known as "spear phishing." Another variation on phishing techniques is the use of the target company's actual Web site as part of the attack. You can expect further refinements and adaptations on the part of phishers.

Malware, spyware, and phishing are just some of the threats present on the Internet. These will be explored in more depth in subsequent chapters. For now, let's examine some of the countermeasures that have been developed to address these threats.

Adaptive Countermeasures to Threats

Internet threats are have adapted to countermeasures. Malware writers create techniques to avoid pattern-based detection. Spyware writers add code to their malware to turn off popular spyware detection programs. Phishers change their scamming messages and target smaller audiences. There is an obvious need to have equally adaptive countermeasures. Countermeasures address the constantly changing threat profile of the Internet in several ways:

- Multiple countermeasures to a single threat
- Improved detection techniques
- Real-time updates of countermeasure databases
- Multi-vector threat protection

Consider antivirus protection on laptops. When connected to a corporate network, scanners deployed on the perimeter of the network can detect and block malicious code before it reaches the laptop. However, when the laptop is used to surf the Internet from home or at a coffee shop, the network protection is not available. In this case, local antivirus protection is essential to prevent malware from infecting the machine.

As mentioned earlier, malware writers have developed techniques to avoid pattern detection by antivirus programs; in response antivirus writers developed entirely new methods of detection. Similarly, firewalls and intrusion prevention systems (IPSs) are improving their ability to detect and block network attacks. Vulnerability scanners are easier to use and have been developed for multiple platforms. The Microsoft Baseline Security Analyzer, for example, provides average Windows users with services once limited to seasoned UNIX administrators.

The Internet is constantly changing. Sites are added and shut down. Threats move from one point to another. There is no practical way for a single business to monitor Internet sites and block potentially damaging content. Instead, security firms and collaborative efforts have been launched to create real-time databases of sites that many organizations would want to block, such as gambling, adult, shopping, hate speech, and other sites unrelated to the business.

Finally, countermeasures, just like malware, have become more sophisticated. Personal use products now combine firewall, intrusion detection, and virus protection. Feature-rich network protection applications can scan email, Web content, ftp transfers, and other traffic to prevent downloading of offensive material and malware while ensuring that private and proprietary information does not leak out of the organization. As adaptive as the countermeasures are, there is no single solution that addresses the full spectrum of security needs with regards to protecting Internet access.

Need for Multipoint Solutions to Internet Threats

Varied threats require varied countermeasures. Although some distinct threats can be addressed with a single tool—for example, both viruses and spam can be detected with pattern-matching content filters—multiple tools at multiple points in the infrastructure are required to create a comprehensive response to Internet threats. The need for multipoint solutions arises from several factors:

- Transmission method of threats
- Methods of attack
- Network architecture
- Manageability of countermeasures

Often countermeasures are deployed to address all of these factors.

Transmission Methods of Threats

Threats are transmitted in a variety of ways. Viruses and blended threats can travel in email and instant messages, and we have recently witnessed the emergence of cell phone malware. Worms propagate by exploiting vulnerabilities in applications and operating systems (OSs). Ironically, Trojan Horses can be intentionally installed by users thinking they are adding useful software to their systems. Content-filtering technologies, both on the desktop and on the network, can counter many of these threats. Vulnerability scanners can help detect weaknesses in applications that might be exploited by worms. Firewalls and IPSs can block and detect anomalous network activity generated by blended threats, Trojan Horses, and other malware that attempts to change system settings or transmit data. Network firewalls and intrusion detection systems (IDSs) have been available for some time, and personal firewalls deployed at the desktop are now commonplace.

Methods of Attack

Once within the secure perimeter of a network, threats attempt to compromise systems. Malware may delete files, change registry settings, increase privileges on compromised accounts, copy data files, record and transmit keystrokes, or even take control of the machine for later use as a "bot" in a network of hacker-controlled devices. Antivirus solutions (which have evolved to be generalized anti-malware systems), IPSs, network content filtering, and firewalls all contribute to countering these threats. Again, both network-based and local deployments of these countermeasures are needed for comprehensive security.

Network Architecture

Not surprisingly, the architecture of the network within an organization can help protect critical assets. Networks are typically segmented for both security and performance reasons. At the very least, networks will use a basic demilitarized zone (DMZ) architecture as Figure 1.2 shows.

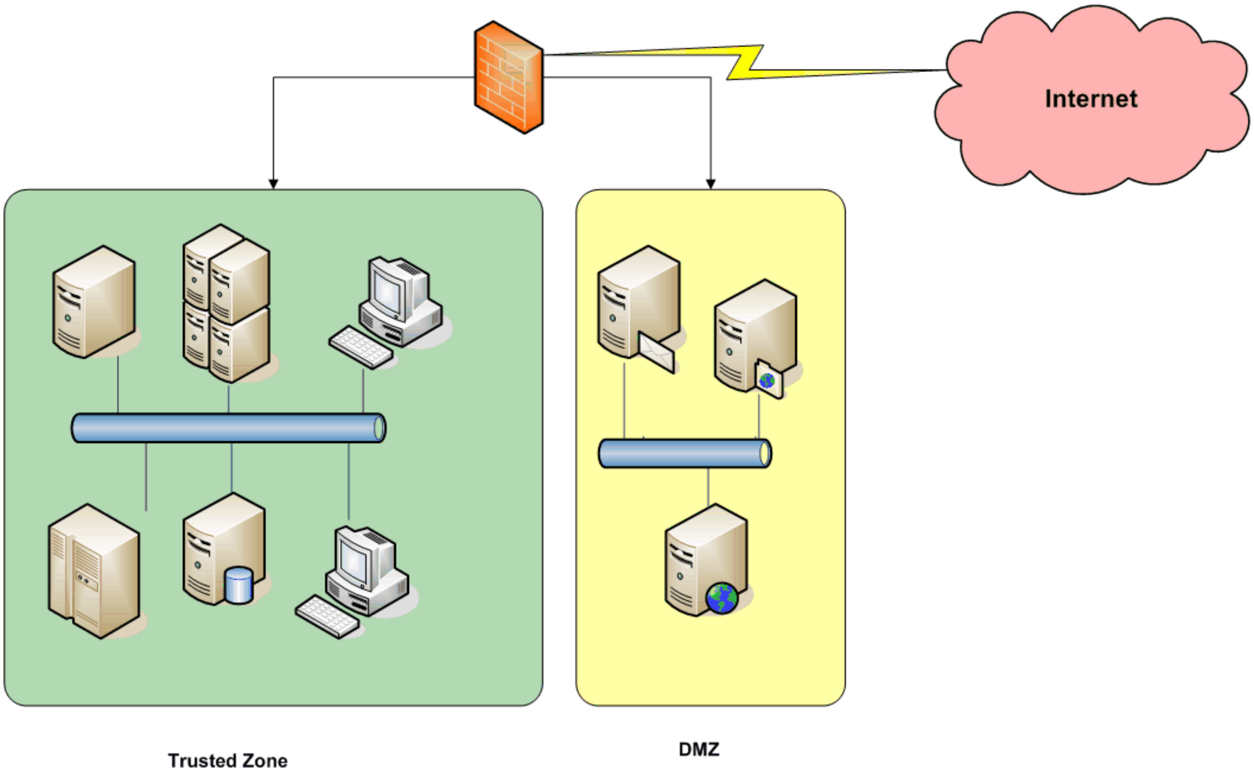

Figure 1.2: Network with a basic DMZ architecture.

Careful design of network architecture isolates traffic and allows for the deployment of countermeasures throughout the organization. For example, large networks might have multiple email servers on different segments. Each of these may have a corresponding content-filtering server or appliance on the segment to ensure adequate performance.

Manageability of Countermeasures

The ability to manage countermeasures is an important aspect of their successful use. In some cases, countermeasures are relatively easy to manage. For example, server OSs can be patched as needed by systems administrators. Of course, there are still change-management issues and questions of when and how long a server can be down, but systems administrators can still control many aspects of the server. Similarly, content filters on the network can be configured to automatically update pattern detection databases on a regular basis. Application managers have complete control. Other countermeasures are more difficult to manage.

Laptop and mobile devices, by their very nature, are not always connected to the network. If a new threat is discovered or a vulnerability uncovered in the OS, system managers cannot push a patch to a laptop that is not connected to the network. Until that device is put back on the network, it is vulnerable.

The most difficult situation occurs when unmanaged devices access the organization's network. Customers, suppliers, and other business partners may access Web applications routinely. Those users' devices could be infected with malware, bot software, rootkits, or other systems that could compromise the organization's network. To counter these threats, the network must monitor and analyze data transmitted to and from these devices.

Countermeasures must be deployed throughout the network to protect against a variety of threats. However, deploying is far from the last step in maintaining these systems. Databases of threat patterns must be updated, the countermeasures themselves must be updated periodically, adequate performance must be maintained, and they must be configured to enforce organizational policies and change as the policies change.

Summary

Preserving the integrity of business Internet access is a multifaceted challenge. There is a clear business case for undertaking the problem, especially in light of compliance and human resource issues that are directly affected by Internet technologies. Although there are many threats to businesses, there are also countermeasures. With a combination of well-defined policies and appropriately deployed and managed countermeasures, organizations can protect the integrity of their operations while leveraging the benefits of Internet technologies.