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 2: Organizational Responsibilities for Protecting the Network from Internet Attacks

Any computer linked to the Internet is potentially subject to a variety of threats. These threats range from less-malicious port scans to disruptive and costly DoS attacks, virus infections, and theft of information. Damage can easily extend beyond a single compromised system.

SQL Slammer disrupted Internet operations around the globe because SQL Server administrators did not patch a known vulnerability. The problem was likely compounded by the fact that some users of Microsoft SQL Server Desktop Edition (MSDE), which is used for persistent storage in some desktop applications, may not have known they were running a version of SQL Server.

Clearly, protecting information assets begins with knowing which systems are in place and how they function; but organizational responsibilities extend to a wide array of challenges, including:

- Protecting employees
- Protecting information assets
- Protecting customers
- Protecting stakeholders

This chapter examines a variety of threats to organizations and describes how to use secure content technologies to manage those threats and their adverse consequences.

Protecting Employees

Employers want to protect employees from disruptions in their work processes. Businesses, government agencies, and other organizations cannot accomplish their objectives if their employees are left idle by downed systems and disrupted services. Although these are real and costly concerns, they are not the only threats to employees. Employees expect and have a right to work in non-threatening conditions. The Internet has created new means for perpetrating the old threats of harassment and hostile work environments. Besides attending to infrastructure protection, employers today are rightfully concerned with protecting their employees.

Harassment in the Workplace

Harassment in the workplace has gained attention in the past several decades, both in the United States and the European Union. Employers are more aware of the problem and many have established practices and procedures to protect employees. Harassment can be physical or psychological in form; it can be constituted by a single event or a series of incidents. In the context of this guide, the question addressed is, How can employers protect employees from harassment and hostile work environment conditions that make use of information technology (IT)?

Recent years have seen the emergence of harassment and hostile work environment incidents in which the use of company computer systems has played a central role. Some of the more well-known court cases in this area include:

- In *Smyth v. The Pillsbury Company*, an employee, Michael A. Smyth, was dismissed for threatening to kill members of the sales management staff in an email to his supervisor sent over the company's email system. (914 F. Supp. 97 (E.D. Pa. 1996))
- In *Bourke v. Nissan Motor Co*, two individuals responsible for establishing an email were dismissed for sending personal messages with inappropriate sexual humor. (YC 003979 Cal. Super. Ct., L.A. County 1991, affirmed by the Court of Appeals in 1993)
- In *May v. Teleservice Resources, Inc*. (WL 222906 (N.D. Tex. 1997)) a manager was demoted to an entry-level position after an email was intercepted that was critical of the companies cultural diversity program.

As technology is playing an integral role in harassment incidents, organizations are faced with questions of how to respond and balance competing interests, such as how to balance the right to be free from harassment with other employees' perceived privacy rights with regards to electronic transmissions. The American Management Association 2003 Survey on email rules, policies, and practices depicts the lack of a single approach to controlling the content of email and the way employees use email. The findings included:

- 52 percent of companies surveyed use some form of email monitoring and enforce email policies with disciplinary actions
- 22 percent of companies surveyed had terminated an employee for violating an email policy
- 75 percent of surveyed companies have formal policies, but fewer than 50 percent of those companies provide training on those policies
- 90 percent of email users receive personal email at work; for most, personal email is less than 10 percent of their total email
- 14 percent of companies surveyed have been ordered by a court or regulatory agency to produce employee email
- 5 percent of companies have been involved in a lawsuit triggered by email use

📖 These statistics are found in American Management Association, 2003 Email Rules, Policies and Practices Survey, available at http://www.epolicyinstitute.com/survey/survey.pdf.

Clearly, companies are responding to the organizational and legal demands brought on by the increased use and importance of email. Establishing formal policies and monitoring compliance are widely practiced. At the same time, not all companies using policies and monitoring train their users on these topics. Employees also continue to use email for personal use although, at least a significant number of them, have been trained on proper use policies. (An earlier survey cited in the *Monthly Labor Review* found both employers and employees comfortable with some personal use of email.)

Are these findings inconsistent? On the one hand, employers want to control how email is used. In addition, the court cases cited earlier demonstrate that employers are willing to resort to litigation to defend their ability to maintain that control. On the other hand, a large majority of employees continue to use email for personal use—action presumably not allowed by most policies. Rather than demonstrating an inconsistency in findings, these results reflect the complexity of the subject.

Email systems should be used only for business use; at the same time, employers recognize the occasional use of email for personal use is not detrimental to the organization. This behavior falls into the same category of making a personal call from a work phone. The goal of email monitoring should be to identify and isolate those instances of improper use that threaten the welfare of other employees or the organization as a whole.

Harassment is a problem that extends well beyond Internet and email use, as is another problem that has co-opted IT—offensive material in the workplace.

📖 Workplace harassment is complex subject with both organizational and legal dimensions. For examples of the breadth and depth of the issue see:

📖 Paul Buchanan's "The Evolving Understanding of Workplace Harassment and Employer Liability: Implications for Recent Supreme Court Decisions Under Title VII" at http://www.law.wfu.edu/prebuilt/LR_v34n1_Buchanan.pdf

📖 Virttorio Di Martino "Preventing Violence and Harassment in the Workplace" http://www.eurofound.eu.int/publications/files/EF02109EN.pdf

📖 Charles J. Muhl "Workplace Email and Internet Use" (Monthly Labor Review, February 2003) at http://www.findarticles.com/p/articles/mi_m1153/is_2_126/ai_100729675

Offensive Material in the Workplace

Closely related to the problem of harassment is offensive material in the workplace. Unlike harassment, which is intentional behavior to intimidate or harm another, offensive material is not necessarily brought into the workplace to harm. For example, two friends could share material which they find humorous and others find offensive. This occurred in the *Bourke v. Nissan Motor Co.* case cited earlier.

The Internet has not created a new problem in this area; it has created a new method for conducting the problematic behavior. It would seem that employers must now educate users on what should be obvious. Elizabeth du Fresne, labor and employment attorney, summed up the problem: "I don't understand why [employees] think they can send racial and sexist jokes via email or download pornography at work. Why they don't understand that the same rules of life apply when they get such material from the Internet and pass it on to others in the workplace, I don't know" (Source: "Ethics in the Workplace—I" at http://www.humanlinks.com/manres/ethics1.htm).

The following list highlights best practices in preventing email from being used for harassment and the distribution of offensive material:

- Define clear policies governing email use—state the types of behaviors (for example, threats, use of inappropriate language, and so on) that are not tolerated
- Educate users about policies
- Filter email content to reduce the chance that harassing messages are successfully transmitted
- Inform users that email is monitored and messages may be blocked
- Although legal issues abound in this area, common sense about public and professional behavior can address many of the remaining issues

Protecting Information Assets

IT professionals are keenly aware of the need to keep operational information systems functioning. Some systems must be available 24-hours a day, 7 days a week with only rare downtimes for maintenance. Administrators trade pagers for "on-duty" times with each other so that someone is available to respond immediately if a system goes down. Business users and executive sponsors are dictating strict service level agreements (SLAs) not only for system availability but also for processing windows. Key operational reports and business intelligence reports must be ready at the start of business each day in some cases. In addition to typical maintenance and change management procedures, systems administrators must secure content that enters a corporate network to reduce the chances of several serious threats, including:

- Virus attacks
- Malicious use of computers
- Wasted bandwidth and storage

Preventing Virus and Other Malware Attacks

The threat of viruses, worms, Trojan Horses, and other types of malware is not news. The change in the severity of attacks and the length of time needed to recover, though, is a trend worth noting.

ICSA Labs, an independent research and certification testing center for information security conducts annual surveys on the prevalence and cost of viruses and other malware. The results of the most recent survey (2004) depict disturbing trends:

- 3.9 million virus encounters on 900,000 desktops, servers, and perimeter gateways in 2004; this statistic reflects 392 encounters per 1000 machines per month (an encounter is any time a virus is found and dealt with; it does not necessarily constitute an infection)
- 6 percent increase in virus disasters (25 or more PCs infected with the same virus at the same time) from the prior year; the increase was from 31 percent to 37 percent of respondents
- Recovery time increased 25 percent or 7 days from the prior year
- Cost of recovery, on average, was $130,000
- 91 percent of respondents felt 2004 was somewhat or much worse than 2003, which had been to that point the worst year on record

> 🕮 For complete details about the ICSA Labs survey, see "ICSA Labs 10th Annual Computer Virus Prevalence Survey" at http://www.trusecure.com/cgi-bin/ct_download.cgi?ESCD=w0206&file=VPS2004.pdf.

The signs of increasing threats of viruses and related malware span several different measures.

Infection Rate

The increase in the number of infections is in spite of improved deployment of antivirus software (see Figure 2.1). 98 percent of respondents reported use of full-time background antivirus software on desktops, up from 89 percent in 2003. The use of antivirus scanning within email gateways also rose, reaching 96 percent from a 94 percent rate in 2003.

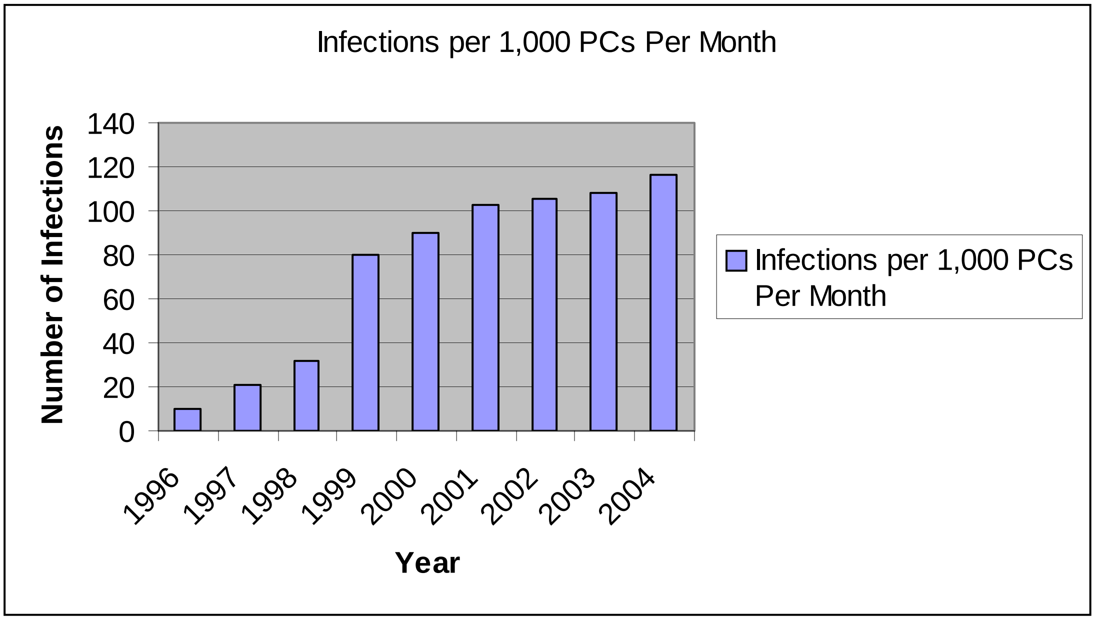

Figure 2.1: The number of infections per month continues to increase (Source: ICSA Labs 10th Annual Computer Virus Prevalence Survey).

Firewall and proxy servers continue to have relatively low protection rates of 50 percent and 60 percent, respectively. As the survey authors noted “perimeter protection provides a critical layer of protection and is a necessary component for a complete corporate virus protection strategy.”

Server Downtime

Servers were included in 95 percent of the virus disasters reported. The average downtime for infected servers was 23 hours with 80 percent reporting recovery within 20 hours (see Figure 2.2).

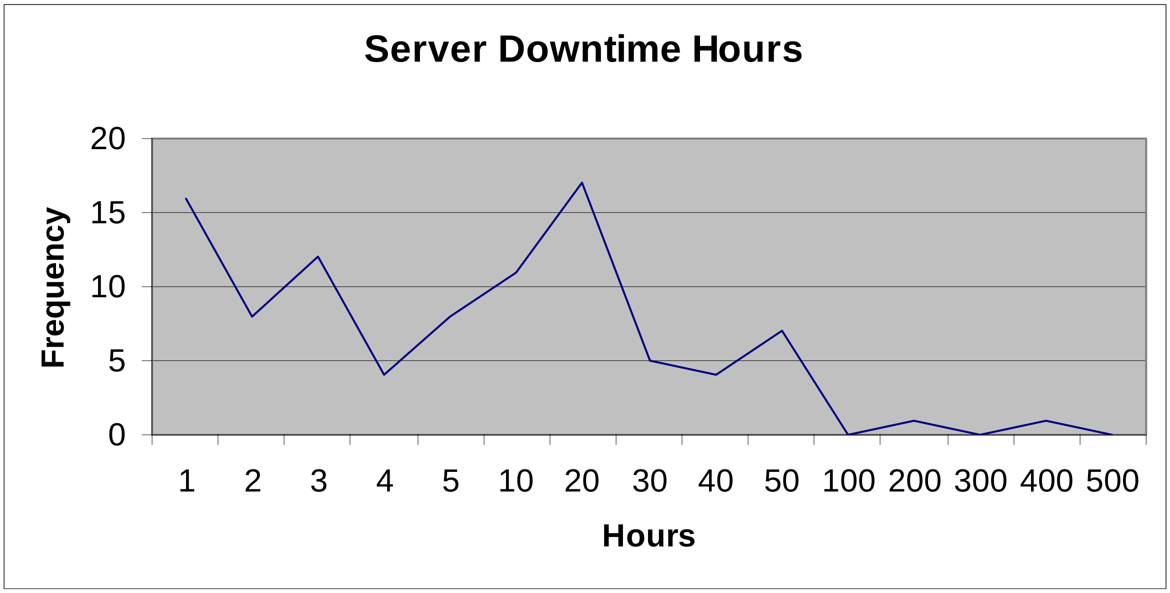

Figure 2.2: Server downtime is typically less than 20 hours per infection (Source: ICSA Labs 10th Annual Computer Virus Prevalence Survey).

The survey notes an upward trend in the time required to disinfect and recover from virus infections.

Recovery Time

ICSA Labs has found that companies are facing more virus incidents—requiring more personnel, resources, and time. The average recovery time in 2003 was 24 person days; in 2004, that figure rose to 31 days (see Figure 2.3).

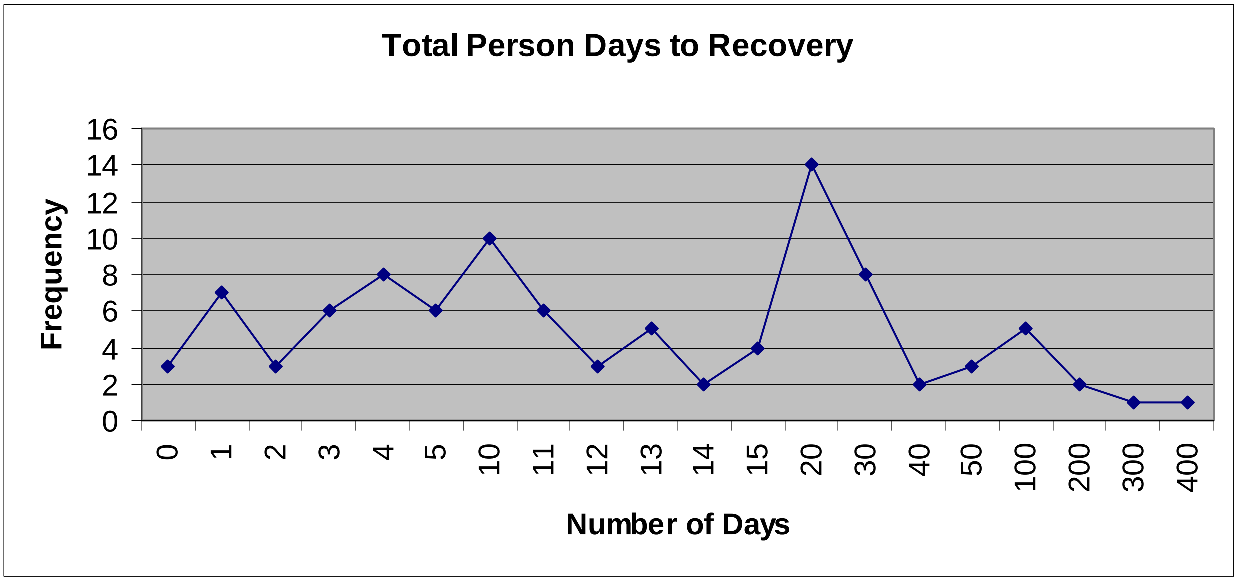

Figure 2.3: On average, 31 person days are now required to recover from an infection (Source: ICSA Labs 10th Annual Computer Virus Prevalence Survey).

Recovery Cost

As Figure 2.4 illustrates, the average cost to recover from a virus disaster in 2004 was $130,000, up from an average of $99,900 in 2003.

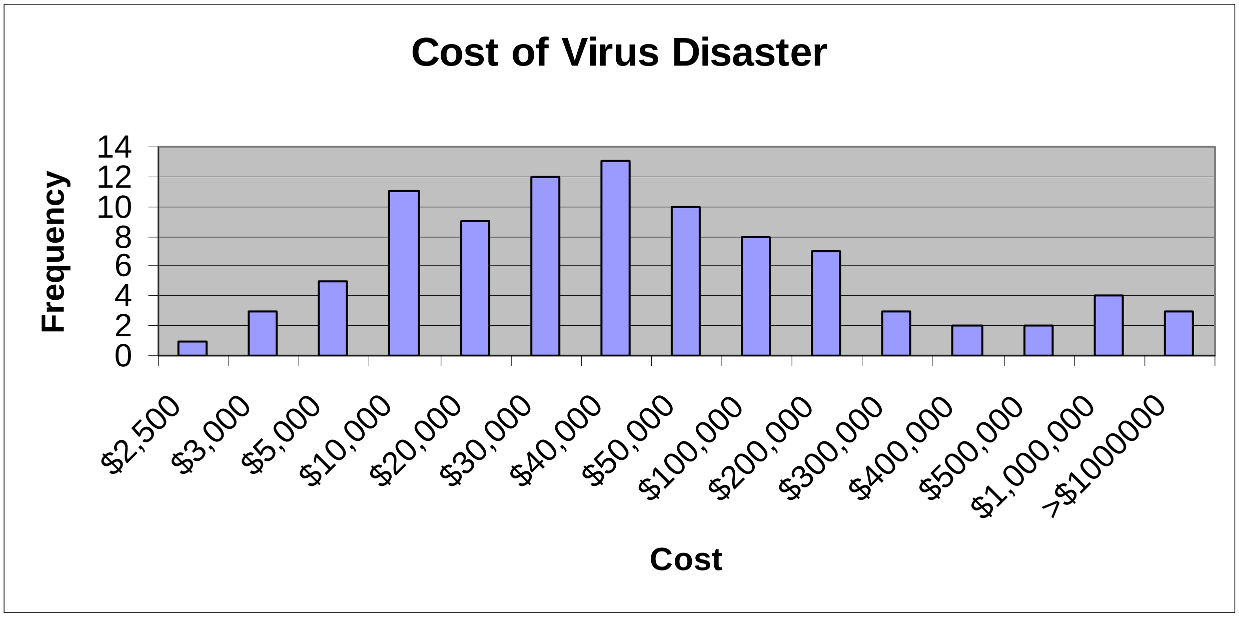

Figure 2.4: The average cost of virus recovery includes both a relatively low number of low cost and high cost recoveries (Source: ICSA Labs 10th Annual Computer Virus Prevalence Survey).

It should be noted, the survey authors estimate that respondents have historically underestimated the cost of recovery by a factor of *7 to 10 times*.

Other Factors and Emerging Trends

In addition to the quantitative measures, the survey authors noted other disturbing trends, including:

- Virus writers and spammers are joining forces or at least adopting each others techniques.
- Viruses that successfully infect systems are using their own email engines for propagating themselves and distributing spam.
- Virus families are surviving longer in part due to rapid deployment of variants.

Although these additional factors make virus protection more difficult, the pattern is not new. Security professionals have long dealt with attackers and cyber-criminals who adapt to improved countermeasures. When early antivirus software successfully used signatures to detect and isolate viruses, virus writers tried encryption and then successfully created mutating viruses to thwart signature-based systems. Antivirus designers responded with a new class of antivirus detection methods based on behavioral analysis. Some emerging variations on traditional attacking and malware distributions include:

- Spammers and virus writers are sharing techniques, so it is not surprising to see antivirus and anti-spam technologies leveraging each other's strengths to counter the ever-evolving nature of virus threats.
- The use of malware is also spreading into other forms of cyber crime.
    - The Turkish authorities, for example, are investigating 16 suspects involved in credit card fraud who have links to the Zotob worm outbreak (Source: Jaikumar Vijayan "Zotob Case May Lead to Credit Card Arrests" http://www.computerworld.com/securitytopics/security/story/0,10801,104388,00.html)
    - Incidence of extortion of online gaming sites with threats of DoS attacks to indicate a linking of organized crime and attackers (Source: Jack M. Germain, "Global Extortion: Online Gambling and Organized Hacking", http://www.technewsworld.com/story/33171.html)
    - In 2000, a variation of the Love Letter worm was used to gain access to passwords at one Swiss and at least two United States banks (Source: Phil Williams, CERT Coordination Center, "Organized Crime and Cyber-crime: Implications for Business" http://www.cert.org/archive/pdf/cybercrime-business.pdf)
- Hacker wars, in which competing individuals or groups modify their own or each other's viruses and worms to gain control of compromised computers

There is no reason to doubt that these emerging trends and evolving threats will be dealt with as earlier threats have been addressed. At the same time, the widespread use of desktop antivirus software has not been enough to halt the increasing threat of viruses, malware, and the emerging threats from organized crime.

Malicious Use of Computers

Some malware is destructive; it may be designed to demonstrate an attacker's abilities or to disrupt services, but it does not have any other purpose. Other malware is designed with the clear intention of gaining control of infected machines and using those systems' computing and network resources for economic gain or to cause service disruptions beyond the compromised machine. Some of the primary reasons an attacker would want to gain control of a computer include:

- Send spam
- Commit click fraud
- Launch DoS attacks

The first two items clearly have economic gain as an objective; disruptive attacks such as DoS attacks, may or may not be economically motivated. Computers that have been compromised are known as zombie computers, or zombies for short.

Spamming with Zombies

Spammers are in business and have the same concerns as other businesses—minimizing costs and maximizing revenues. They can minimize their costs by using some one else's computers and bandwidth to distribute email. Fortunately for the spammers, that same technique helps them maximize revenues. By increasing the number of zombie computers under their control, they can increase the amount of spam they generate, which, in turn, leads to higher revenues (see Figure 2.5). There are more than economic incentives as well.

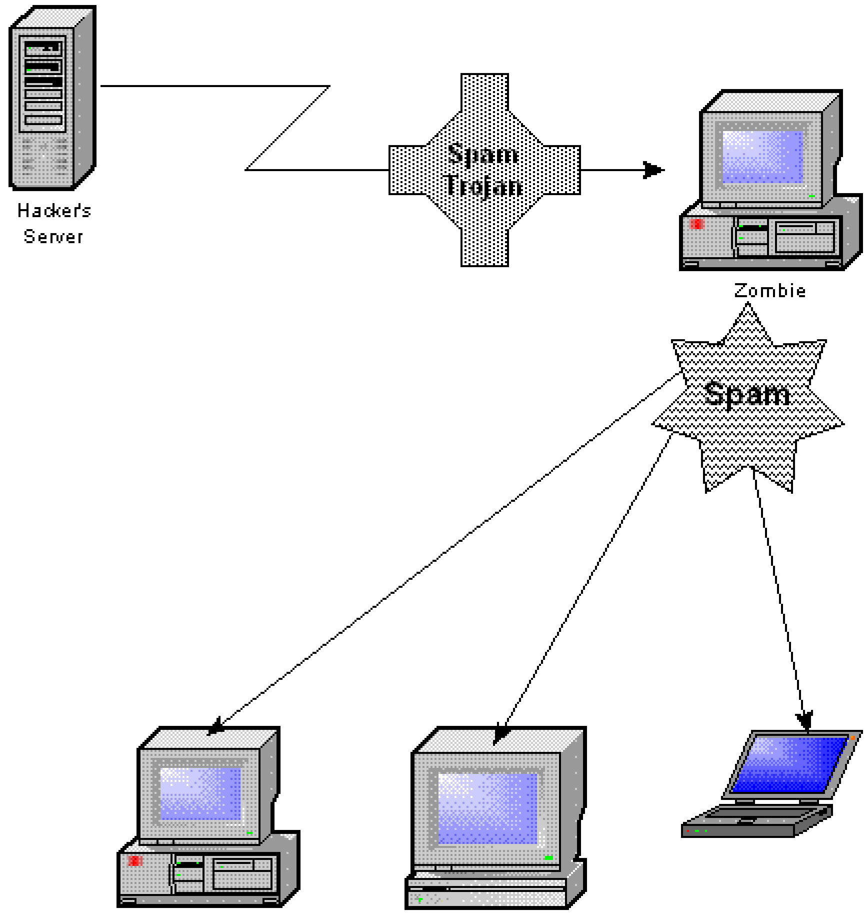

Figure 2.5: PCs are first compromised by a spam Trojan Horse, virus, or other malware; the infected machines then become email servers for spam distribution.

Spammers violate the law when they send mass mailings of unwanted, unsolicited emails. In the United States, the federal government and 38 states have passed anti-spam legislation. The European Union, Australia, and other countries have also passed laws regulating spam. Needless to say, spammers have a lot of incentive to mask their identities. Zombies can help with that.

📖 For links to the text of anti-spam laws, see http://www.spamlaws.com/.

Using zombies also helps spammers avoid domain black lists such as DNS Providers Blacklist and real-time spam blacklist services (RBLs). As the mass mailings are spread out to a large number of computers on different domains, spammers can send large volumes of email without necessarily exceeding thresholds that would trigger their classification as a spammer.

If someone were to trace the origin of a piece of spam, it would lead to the compromised computer, not to the spammer. For example, Tom Spring, a writer for *PC World*, traced spam messages he received back to a number of legitimate businesses and organizations, including a financial planning company in New York, a medical services company in Kansas, a nursing home in Ontario, and a university in Beijing (Source: Tom Spring, "Slaying Spam-Spewing Zombie PCs" at http://www.pcworld.com/news/article/0,aid,121381,00.asp). Spammers are using techniques developed by attackers for distributed processing, such as distributed DoS (DDoS) attacks, to capture computing resources while hiding their identities.

Responding to Spam Zombies

The problem of zombies distributing spam has become so prevalent that email and network systems administrators are heeding calls to do more. Countermeasures are being deployed at two levels:

- Internet service provider (ISP) level
- Corporate network level

Some have argued that ISPs must do more to stop spam. As spammers develop more sophisticated techniques, it is becoming less likely that average users can keep up with the technical knowledge required to protect their computers. One anti-spam measure that has been advocated at the ISP level is blocking outbound traffic on port 25, the port used for email. There are advantages and disadvantages to this approach.

Normally, when a user sends an email, the message is sent via port 25 to an email server at an ISP or corporate email server. The email server then relays the message to the target recipient. This process works well for those of us sending moderate amounts of email and not trying to hide our email activity. Spam programs that infect zombie computers typically use their own email engine and bypass the ISP or corporate email server and send mail directly to the recipient. In response, many in the industry have argued that blocking port 25 can reduce the impact of zombies sending spam.

The advantages of this approach include:

- Most users that send large volumes of email via port 25 are not aware if they are spamming and would likely welcome the preventative measure
- Users with a legitimate need to use port 25 could be granted access if they agree to reasonable terms of use (for example, no mass mailings)
- Blocking port 25 shifts some of the responsibility for controlling spam closer to the point of origin and away from the recipient

There are disadvantages to blocking port 25, including the fact that completely blocking port 25 is probably not practical and additional administrative overhead will be incurred managing exceptions, and blocking port 25 at the perimeter will still allow spamming within the organizational network.

There is also the defeatist argument that spammers will just find away around port 25 blocks. If this problem follows the pattern of threat-countermeasure-response with revised threat that has characterized information security since its inception, you can certainly expect some workaround to this countermeasure. However, anti-spam researchers and practitioners will develop a countermeasure for the spammer’s response. And so the cycle will continue.

📖 See Larry Seltzer’s “Shutting Down the Internet Highway to Hell” at http://www.eweek.com/article2/0,1759,1784276,00.asp and Joe St. Sauver’s “Spam Zombies and Inbound Flows to Compromised Customer Systems” http://darkwing.uoregon.edu/~joe/zombies.pdf for a discussion from both sides of the port 25 blocking debate.

Anti-spam measures can be deployed within the corporate network as well:

- Personal firewalls—Although contributing to the overall solution of reducing spam, each of these options serves a different purpose. Personal firewalls examine network traffic to and from a desktop or laptop. A personal firewall brings the same type of protection that traditionally has been found at the perimeter, including blocking ports and filtering by protocol. In addition, personal firewalls can provide ease of use features for non-technical users, such as pop-ups indicating a program is trying to access the Internet. If the user is not sure whether the program should be accessing the Internet, for example a spam Trojan Horse, its traffic can be blocked by the firewall.
- Content filtering—In cases in which spam reaches the corporate network, either as incoming email or as outgoing messages from a zombie, a content filtering appliance can block the traffic.
- Desktop anti-spam software—Desktop anti-spam software, like desktop antivirus software, is designed to protect a single computer. Desktop protection is especially important for mobile devices that are not always protected by network-based content filtering.

The combination of personal firewalls, content filtering, and desktop anti-spam software are one example of a defense-in-depth strategy that provides multiple types of countermeasures.

Committing Click Fraud with Zombies

Online advertising is an important source of revenues for Web publishers and search engines such as Google and Yahoo. Publishers typically charge advertisers for each click on an ad displayed by the publisher. This setup can create an incentive to fraudulently increase the number of clicks on an advertisement. Click fraud is committed in one of two ways: either a human clicks on ad links or a script programmatically simulates a click. As with spam delivery, fraudulent clicks are easier to hide if they are coming from a large number of compromised machines.

> 📖 The Times of India documented a case of organized click fraud in which a fraud group hired staff whose job was to click online ads for $0.18 to $0.25 per click; for more information, see http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms.

A variation on click fraud, known as impression fraud, is emerging. In this scheme, the defrauder temporarily terminates online ads with a search engine. He then proceeds to query the search engine in such a way that competitors' ads are displayed. The defrauder's script does not click the competitors' ads, so the competitors' click-through rates drop. Lower click-through rates can adversely impact the competitors' ad position or reduce the cost the defrauder must pay for a particular position.

Search engines and online advertisers are implementing anti-click fraud technologies, but this type of incident provides yet another example of how the infrastructure of e-commerce can be exploited for fraud. A key component of some of the schemes is the ability to distribute programs that commit the fraud using zombie computers, thus allowing the perpetrators to hide their identities.

Spamming and click fraud have clear economic motives. The economic benefit of exploiting compromised machines is not always so obvious.

📖 For more information about click fraud and related schemes, see Jessie Stricchiola's "Lost Per Click: Search Advertising & Click Fraud" at http://searchenginewatch.com/searchday/article.php/3387581.

DDoS Attacks

A DoS attack occurs when a malicious program sends excessive network traffic to a server in an effort to consume the server's key resources so that the server cannot respond to legitimate requests. A DDoS attack originates from multiple machines. A simple form of this type of attack is known as SYN Flooding.

For example, two devices on the Internet begin communication with a three-step process. The initiating device sends a synchronization packet (SYN) to the recipient. The recipient machine responds with a synchronization acknowledgment packet (SYN/ACK) if a service is available on the port or a reset packet (RST) if the port is closed. The initiating machine would then respond with an acknowledgement packet (ACK) after receiving the SYN/ACK packet, and communications would proceed (see Figure 2.6).

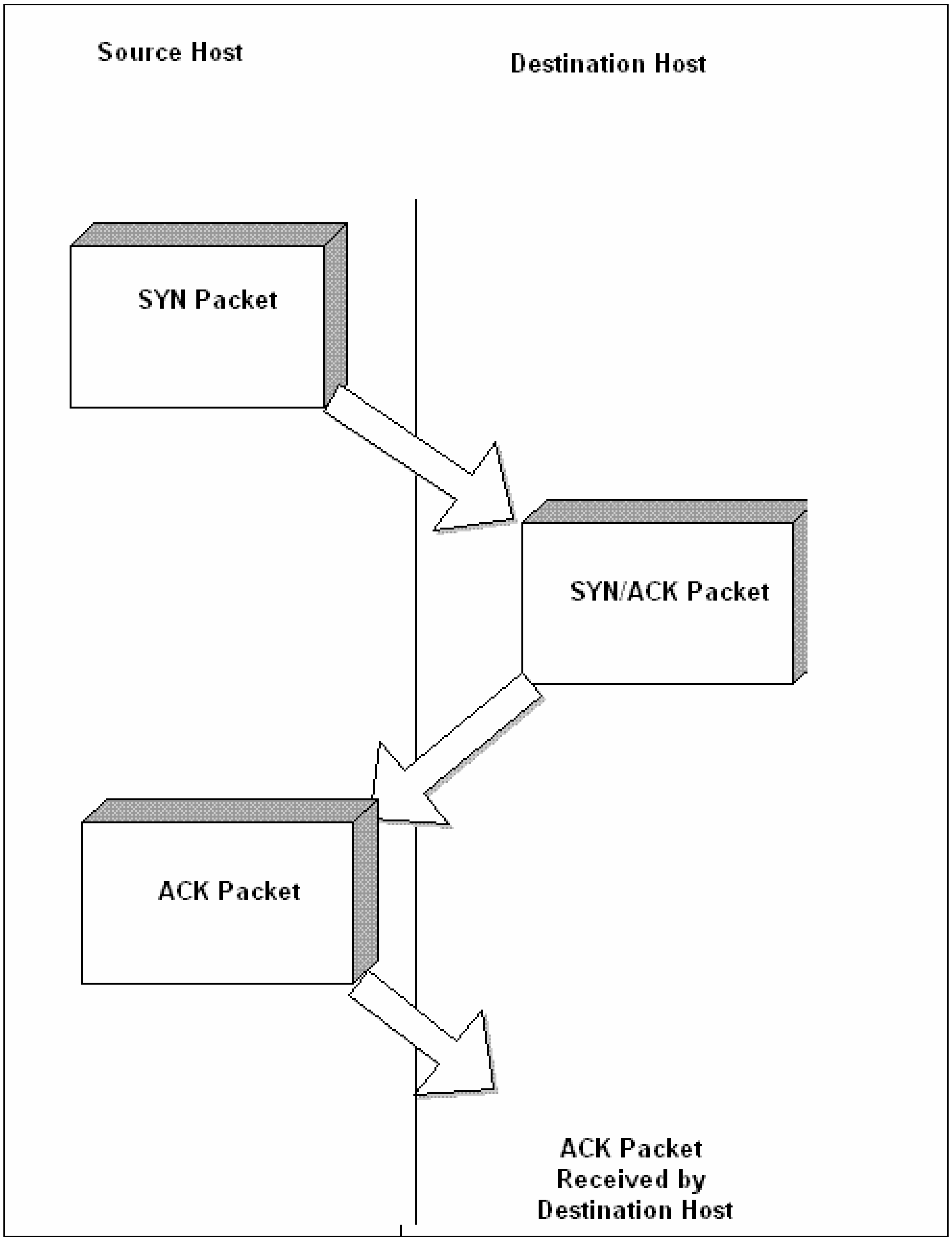

Figure 2.6: TCP communications begins with a three-way handshake.

When a SYN packet arrives, it contains the return address of the sender of the packet. The destination host uses this address to send the SYN/ACK packet. In addition to sending the packet, the destination host allocates a connection for its pool of network connections to this session. There is a limit to the number of connections maintained, and once those connections are used, new requests (SYN packets from other hosts) are refused. When sessions terminate, connections are freed and available for use by other hosts.

SYN Flooding exploits the fact that the destination host trusts the source host to provide its legitimate address. Instead, the attacking program uses a false, typically random, address. The destination host then sends the reply packet (SYN/ACK) to a false address and waits for a response (see Figure 2.7). While the destination waits for the ACK, a connection is tied up and will stay that way until the session is killed (the time to wait is system dependent, it may be a few minutes).

An attacker can easily initiate enough sessions to consume all the connections in the pool and continue to initiate new sessions as connections become available. Again, compromised computers can play a key role. A zombie with a DoS program can be the source of SYN packets that flood a destination host.

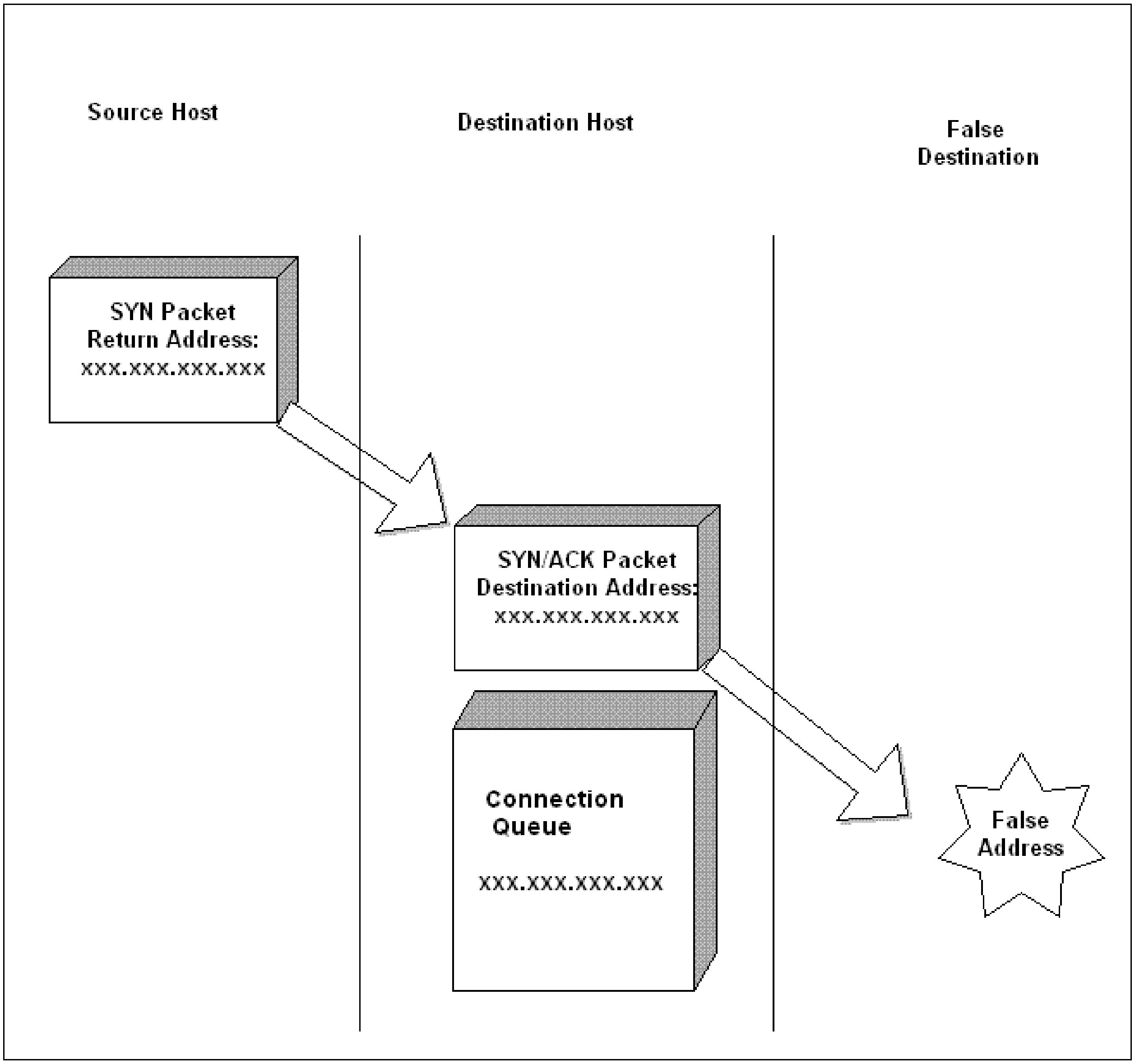
Source Host
Destination Host
False Destination
SYN Packet Return Address: xxx.xxx.xxx.xxx
SYN/ACK Packet Destination Address: xxx.xxx.xxx.xxx
Connection Queue
xxx.xxx.xxx.xxx
False Address

Figure 2.7: SYN Floods fill the connection queue while the destination host waits for acknowledgments that will never arrive.

DoS attacks can be prevented by denying perpetrators devices for launching those attacks and blocking traffic on corporate networks that could be used as part of DDoS attack. Ideally, a DDoS program would never make it to a corporate device. Network-based content scanning and desktop antivirus programs can detect and quarantine these malware programs along with others. In addition, firewalls can be configured to prevent outgoing traffic with false IP addresses.

> 🕮 For more techniques for preventing DoS attacks, see the SANS Institute's step-by-step guide to preventing these types of attacks at http://www.sans.org/dosstep/.

The malicious use of compromised computers is a serious threat to computer and information security. Spamming, click fraud, and DoS attacks are three examples of how compromised computers can be exploited. Other types of attacks are likely to emerge that exploit vulnerable servers and desktops. Clearly, the need to scan incoming and outgoing content will not diminish and will likely increase in the future. In addition to the malicious use of computers, information assets are threatened with wasted resources.

Preventing Wasted Bandwidth and Storage

Another threat to corporate and organizational information assets is wasted bandwidth and storage. Small and midsized businesses may pay between $400 and $550 per month for a T-1 (1.544 megabits/second) Internet connection; while large organizations can pay between $4000 and $16,000 per month for a T-3 (43.232 megabits/second) line (Source: Infobahn, http://www.infobahn.com/research-information.htm). Malware and spammers can hit an organization coming and going, literally.

Incoming spam consumes bandwidth, and the longer the spam travels before it is detected, the more network bandwidth is wasted (see Figure 2.8). Ideally, ISPs would block spam near its point of origin. The next best option is to block spam as it reaches a corporate network. Network appliances positioned just inside of a firewall can meet this objective. The next point to catch spam is at the email server, but this method taxes the email server with additional work. The last chance to catch spam is at the desktop, but at that point, there is no savings on wasted bandwidth.

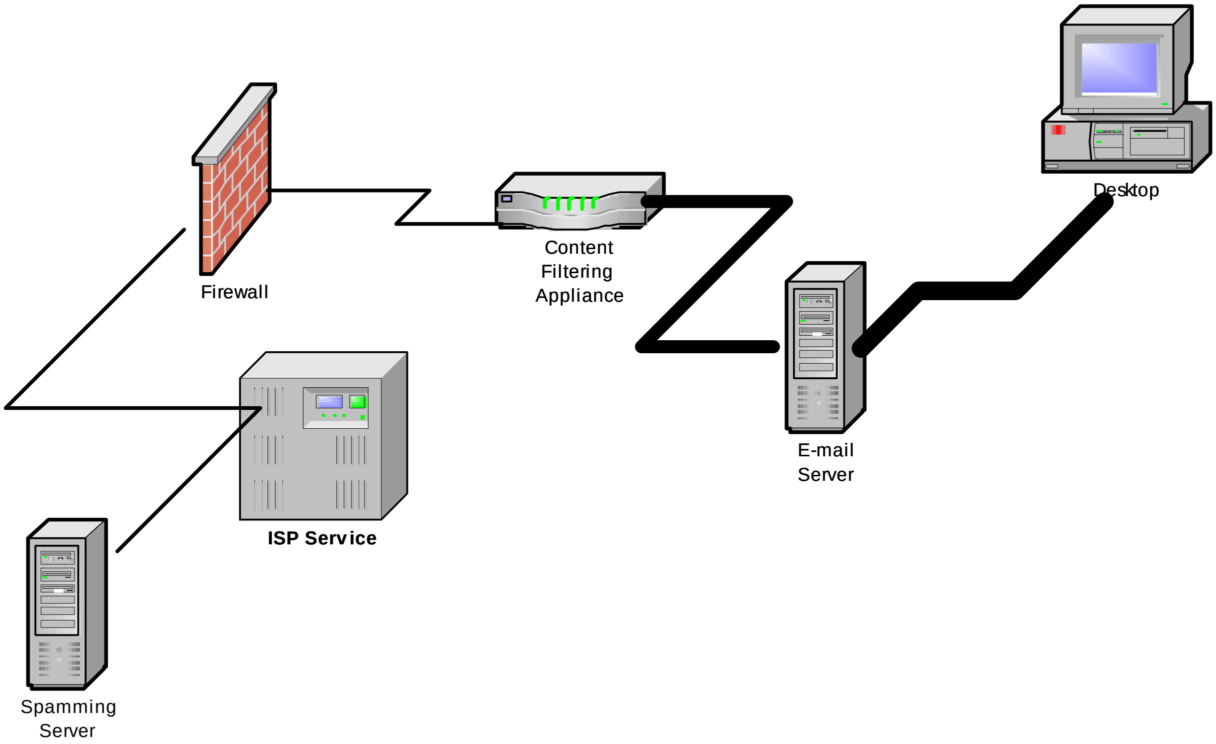

Figure 2.8: The longer spam travels from its point of origin to the recipient, the more bandwidth is wasted.

An internal device infected with a spam distribution program can generate substantial volumes of outgoing mail messages that consume bandwidth as well. Malware that implements DDoS attacks or click through fraud or spreads malware (such as SQL Slammer) also consumes bandwidth unnecessarily.

Spam and Unnecessary Storage

Like bandwidth, storage is a resource that can easily be consumed by spam. Unlike bandwidth, the waste of storage space continues through time. The problem may be compounded by email policies:

- Spam is stored in an email server and may be duplicated on the recipient's local drive.
- Depending on an organization's email retention policy, spam may be backed up onto long-term storage.
- In highly regulated or litigious industries, archives may be kept for long periods of time, sometimes in costly, off-site storage facilities.

Once a piece of email reaches an email server, the message becomes subject to email policies that must address a wide range of issues, such as auditing and compliance. Courts may demand that litigants produce emails during the discovery phase of a trial. These considerations can lead some organizations to back up and keep emails, including spam, for long periods of time. Again, as with wasted network bandwidth, it is best to detect and remove spam as early as possible in the transmission process. Ideally, spam will never reach the recipient's email server; that would save both the recipient and the company time, money, and management headaches.

Information assets must obviously be protected; what is less obvious is the ways in which malware and spam can harm those assets. In the early days of PC use and widespread Internet adoption, viruses would be created and distributed just to cause destruction. Today, economic incentives, from boarder-line legal spam to organized criminal activities, are exploiting vulnerabilities in technology and business processes and driving innovative threats. The trend will continue.

Protecting Customers

Organizations carry varying degrees of regulated responsibility in protecting customer information. Healthcare providers are under some of the strictest regulations to keep protected health information confidential. Financial institutions are also subject to regulation as well as market pressures to maintain adequate security for customer data.

No business wants to be the next company to make headlines with a security breach leaving customer information vulnerable. Some recent examples include:

- ChoicePoint, a credit information vendor, allowed unauthorized access to 145,000 customers' addresses and Social Security numbers
- 300,000 individuals may have had their personal information stolen from Lexis-Nexis
- UPS lost a box of CitiGroup's computer tapes with personal information on 3.9 million people
- CardSystem Solutions exposed 40 million credit card customers to fraud and identity theft; the breach cost the company two of its major customers, American Express and Visa

The key obligations of businesses and government agencies with personal information are twofold:

- Prevent the disclosure of confidential information
- Prevent identity theft that results from disclosed information

Accomplishing these objectives is not a trivial task in today's interconnected environment.

Preventing Disclosure of Confidential Information

What is confidential information? In the absence of regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), that explicitly define confidential information, the question is difficult to answer. One customer may not mind a business or non-profit sharing their name and address with similar or related organizations while another might consider it a breach of his or her privacy. Opt-in programs are widely employed to allow customers to decide themselves how their information is used.

Opt-in and opt-out programs allow businesses to categorize their customers and use their data appropriately. In practical terms, though, there are a number of security issues that still present problems. Customer data is typically consolidated into a single database; it is not separated into opt-in and opt-out databases. Confidential information is intermingled with non-confidential information. Practically speaking, administrators need to protect a database according to the most sensitive information in it. In the case of opt-in and opt-out data in the same database, it all must be treated as confidential. This means:

- Access controls must be in place to limit users' ability to view and change the data
- Audit controls should be in place to track all changes
- Measures must be in place to preserve the confidentiality of data in transit
- Database servers and application servers with access to data must be configured securely

These measures, in addition to other security measures such as vulnerability testing and perimeter defenses, are essential to preventing identity theft.

Protecting Customers from Identity Theft

Identity theft is difficult to prevent when confidential information moves beyond the managed network. For example, when a customer uses an ATM at the bank, the customer is reasonably assured that no malicious programs are running on the machine. What about a public access machine in the local library or in a hotel business center? Chances are good that some type of spyware, keylogger, or video frame grabber may be running on the machine.

Regardless of the defenses and countermeasures put in place in a controlled network, once the data leaves that network, it is subject to disclosure. Security procedures and techniques deployed within a corporate network, including content scanning for malware, can reduce the chance of identity theft and disclosure of confidential information. However, such measures are not enough.

Users—whether employees, contractors, business partners, or customers—should be made aware of vulnerabilities in Internet-based applications. This argument is not in favor of excessive detail about technical vulnerabilities (for example, the database listener module used by Java Database Connectivity—JDBC—is vulnerable to a buffer overflow attack) but for education about best practices such as:

- Clearing buffer caches
- Running antivirus and anti-spyware programs
- Avoiding Internet utilities that could contain Trojan Horses
- Not using public access devices to transmit confidential information such as bank account numbers
- Being conscious of social engineering ploys to disclose confidential information

Identity theft is a problem exacerbated by poor information security but it is not caused by poor security. Preventing identity theft will require a combination of technical and non-technical countermeasures.

Protecting Stakeholders

The last area that organizations must consider with regard to their responsibilities in information management is organizations' stakeholders. Stakeholders can be owners, staff, business partners, and others who contribute to and stand to benefit from the organization's activities. Although there are many ways in which to protect stakeholders interests, the following list highlights three common examples:

- Preventing non-business Web activity
- Complying with regulation
- Avoiding the cost of recovering from security breaches

This list is certainly not comprehensive but is sufficient to demonstrate the scope of the issue facing businesses, government agencies, and other organizations.

Preventing Non-Business Web Activity

Non-business Web activity, beyond a reasonable amount, is a productivity drain. Like the occasional personal phone call at work, a quick check of the weather or last night's sports scores is commonplace and expected in the workplace. Non-business activity becomes a problem when it extends beyond the bounds of reasonable practices to include:

- Protracted periods of browsing. No can reasonably expect to come into work and sit at their desk reading the paper for an hour to be tolerated as reasonable behavior. Similarly, organization's can expect their staff to refrain from perusing an assortment of news sources or spending hours at an online casino.
- Downloading large files for personal use. Businesses and large organizations have large-capacity Internet connections to meet their needs. This connection should not have to be dedicated to downloading music files, video clips, and other forms of entertainment for employees who have slower connections at home.
- Bringing offensive material into the organization. This topic was addressed earlier in the section on protecting employees from hostile working conditions.
- Using corporate assets without permission. For example, downloading a peer-to-peer file-sharing client onto a company computer for sharing non-work related files.

The Internet is a powerful tool for getting work done efficiently but it can also be a distraction. The long-term interests of stakeholders dictate that some policies and procedures must be in place to balance the benefits of the technology with the unwanted costs of non-business–related activity.

Complying with Regulation

Compliance is a hot topic. Scandals of the last decade have demonstrated that not all businesses conduct themselves according to implicitly agreed upon manners and the rules must be explicitly stated. The Sarbanes-Oxley Act, Graham-Leach-Bliley Act, HIPAA, and a host of other regulations now dictate more requirements than previously imposed on organizations. Many of these regulations have implications for the way information systems are deployed, utilized, and managed.

The details of these and other well-known regulations vary, but several basic principals apply across regulations:

- Information must be accurate
- Changes to information must be done according to established procedures
- In many cases, information is confidential and must be treated as such
- Organizations must be able to demonstrate compliance with these regulations

From the perspective of information security, data must be protected from unauthorized tampering (for example, viruses and other malware should not be able to change details of a person's credit history), unauthorized disclosure (for example, millions of credit card holders should not have their information transmitted to an unauthorized destination), and audit logs must be tamperproof (that is, an attacker should not be able to install a root kit to hide the changes he or she made to a system).

Avoiding the Cost of Security Breaches

Recovering from a virus infection or cleaning up Trojan Horses that are generating spam can be costly. These efforts take the time of IT professionals, many of whom are already working at capacity on production operations or new development projects. Even more difficult to quantify is the damage to corporate image and brand when a breach is well publicized. The case of CardSystem Solutions, a credit card transaction processor, is one of the most telling examples of just how much damage a single breach can cost.

Stakeholders have wide and varied interests. From protecting the production capacity of an organization to complying with government regulation to protecting corporate image in the marketplace, stakeholders' interest encompasses the interest of the organizations in general.

Summary

Corporate networks connected to the Internet are capable of delivering great value to organizations. They are also subject to numerous, constantly evolving threats. Organizations have responsibilities to there employees, customers, stakeholders, and themselves to protect their information assets. Fortunately, the tools are available to meet these challenges, as we'll explore throughout the rest of this guide.