Security Guide for Small Business

Enhance your
computer and network
security
today

Microsoft®
Your potential. Our passion.™

Tell Us What You Think.

We would like to know your opinion of this Security Guide and whether you were able to implement any of the security measures recommended. Simply visit **www.securityguidesurvey.com**, answer a few short questions, and we'll send you a free copy of the *Small Business Tips & Templates Toolkit**. This two-CD toolkit provides a rich set of templates, business articles, how-to videos, and tips to help maximize your productivity.

Microsoft® Small Business Team

** Offer good in the U.S. only until 12/31/05 while supplies last. Limit one CD per customer. Please allow 6-8 weeks for delivery.*

From the ASBDC

Dear Small Business Owner:

More small businesses today use networks and the Internet as vital business tools than ever before. While connectivity is indispensable for achieving business success, being more connected also means being more vulnerable to outside threats. Larger companies have security experts at their disposal, but small business owners must make their own decisions about how to secure their networks.

Therefore, I am delighted to introduce the Security Guide for Small Business—a security guide developed by the Microsoft Small Business Team. This guide does an excellent job of explaining why security is important to your business and outlining steps that you can take to improve the security of your network. These steps are not overly difficult, expensive, or beyond the ability of those savvy enough to be running their own businesses.

Sincerely,

Donald Wilson
President & CEO
Association of Small Business Development Centers

Small Business Development Centers

The Small Business Development Center (SBDC) network is a partnership program uniting private enterprise, government, higher education, and local nonprofit economic development organizations. The SBDC network is the U.S. Small Business Administration's largest economic development program, utilizing federal, state, and private funds to provide management and technical assistance to help Americans start, run, and grow their own businesses. With nearly 1,000 centers across the nation, the SBDC program meets the in-depth counseling and training needs of more than 650,000 small businesses annually in face-to-face counseling and training events. The SBDCs across the country are represented by the Association of Small Business Development Centers (ASBDC). To learn more about the ASBDC, visit www.asbdc-us.org

Microsoft Small Business Center

Microsoft Small Business Center is an online resource designed specifically to address the needs of small businesses by demystifying technology and helping small business owners get the most out of their software. To learn more, visit www.microsoft.com/smallbusiness/

From the Microsoft Small Business Team

Dear Small Business Owner:

New security issues such as viruses, hackers, and worms come to light in news articles every day and underline the importance of taking preventative measures. These are serious threats with serious consequences. Yet, many small businesses have not taken the steps to safeguard their businesses. In some cases, it's a matter of limited resources. But, in most cases, small business owners are simply unclear as to what steps they should take or even where to start.

The Security Guide for Small Business explains what you need to do to improve the security of your business. It was written expressly for the small business owner, not the computer guru, and breaks down the major security threats that your business faces. While subjects do involve technical details, we present the issues in everyday language and provide additional details for deeper discovery.

The Microsoft Small Business Team, in partnership with the ASBDC, is delighted to bring you the Security Guide for Small Business to help you secure your business. Start implementing some of these best practices in your business today.

Sincerely,

Cindy Bates
General Manager, US Small Business
Microsoft Corporation

Contents

Is This Guide Right for You?

Computer and online security is a growing concern for businesses of all sizes. Computer security issues range from viruses to automated Internet attacks to outright theft, the result of which is lost information and lost time. Security issues pop up in news articles every day, and most small business owners understand that they should take steps to better secure their businesses. Increasing security can seem complicated, though, and it's often difficult to figure out where to start. This guide helps answer those questions.

If you own a small business or are responsible for directing the computing and security policies for a small business, this guide is written with you in mind. While the subjects covered in this guide are sometimes technical, we try to present the issues in everyday language and then show you where you can find more technical information when you need it.

This guide breaks down the major security threats that your business faces and features a quiz that introduces concepts to help shape the way you think about your own security practices. You'll find a checklist you can follow to increase security (see the sidebar, "Seven Steps to Better Security," for a quick review of these steps, and read the section, "Seven Steps to Better Security," later in this guide for a detailed look at the checklist) and advice for creating a comprehensive security plan of your own. We have even included a sample security plan for a fictitious company named Adventure Works.

While many of the steps outlined in this guide are steps that you can take yourself, don't be afraid to ask for professional support if you need it. Many qualified technology and security consultants are available to help. Be sure to read the section, "Finding the Right Consultant," for information about where to look and what questions to ask.

Seven Steps to Better Security

1. Protect Your Desktops and Laptops
2. Keep Your Data Safe
3. Use the Internet Safely
4. Protect Your Network
5. Protect Your Servers
6. Secure Your Line-of-Business Applications
7. Manage Computers from the Server

What You Need to Know About Security

To understand the threats that exist and how to mitigate them, you need to know some technical stuff. Don't worry—we'll keep it to a minimum.

Many small business owners believe that they do not need to worry much about computer and online security. "After all," they reason, "who would want to target my business when there are so many bigger targets out there?" While it's true that small businesses are not directly attacked as often as larger organizations, there are three reasons why small businesses should be concerned:

- **Small businesses often end up affected by larger attacks, such as mass worm outbreaks or efforts to harvest credit card numbers.**
- **Security is becoming tighter than ever at larger companies, so small business networks look increasingly tempting to attackers.**
- **Not all security threats come from outside your organization.**

Regardless of how or why your business is attacked, recovery usually takes significant time and effort. Imagine if your computer systems were unavailable for a week. Imagine if you lost all the data stored on all the computers in your company. Imagine if your biggest competitor was able to obtain a list of your customers along with sales figures and sales notes. How long would it take before you noticed? What would these breaches cost your company? Could you afford these losses?

It seems like common sense. You wouldn't leave your building unlocked at night. The same is true with information security, and a few simple steps can make you a lot less vulnerable. Technology experts have a way of making basic security seem like a huge and difficult issue. Luckily, securing your business is easier than you might think.

Of course, there is no way to guarantee 100 percent security.

However, you can achieve a high level of security and be prepared in case breaches happen. Properly weighing risks and consequences against the cost of prevention is a good place to start. This section provides an overview of some common computer networking and security-related terms to help demystify the world of computer security.

Networks, Internets, and the Internet

One computer on its own is a beautiful thing—a technical marvel. But it's good to communicate. Link two or more computers together using network cards and cables (or a wireless setup) and you have a local area network (LAN). All the computers on the network can share data and e-mail as well as access shared resources like printers, modems, or broadband Internet connections. Link two or more LANs together and you have a wide area network (WAN). For example, you might link two offices in different locations with a dedicated leased line.

An internet (note the small "i") is a network of networks. Information from any computer in any given network can travel over the internet to any computer on any other network, with the internet acting as a sort of common carrier. Think of an internet as a highway system that links local roads.

The Internet (note the capital "I") is a global internet. All computers on the Internet communicate using standard protocols so that information from any computer on the Internet can reach any other computer on the Internet. Here is where the trouble occurs. Until you connect with a public network, you are reasonably safe from external threats. Hooking up to the public Internet is like publishing your name, address, and phone number and saying, "Hey, look: We have computers here."

Did You Know?

Internet-related fraud was the subject of 55 percent of the more than half-million complaints filed in 2003, up from 45 percent a year earlier, according to the Federal Trade Commission. The median loss for victims of Internet-related fraud was $195.

Packets

Information typically travels across networks in packets. A packet is a chunk of data plus an address and other information that tells the network where to deliver that data. Everything going over the Internet is broken down into packets: Web pages, e-mail messages, downloads, everything. Think of it like taking a circus on the road. You can't take the whole circus in one vehicle. You have to break it up, package it into separate vehicles, tell each vehicle where it's going, and put the circus back together when all the vehicles arrive at their destination. Data traveling over a network works like this, too. Big data is broken down into a series of packets and reassembled at the destination. As packets travel over the Internet, they are effectively exposed to eavesdropping by the public.

Ports and Addresses

Each computer on a network is assigned a unique number called an IP address. The IP address uniquely defines that computer on the network and provides directions for packets to reach their destinations. IP addresses work much like street addresses. Part of the address identifies the network segment of the destination computer, and part of the address identifies the actual computer.

While an IP address refers to a computer and the network on which that computer exists, the individual applications on that computer must also be identifiable. Think of this setup like an apartment number attached to the street address: the street address denotes the apartment building, and the apartment number denotes the actual apartment. The IP address denotes the computer, and the port number denotes the program on that computer. Each program on a computer that must send and receive data over the network is assigned a special port number. When packets of information are received at a

particular port, the computer knows which application gets the packet. For example, port 80 is the port for Web servers (which host the websites you use your Web browser to explore), and port 25 is the port that is used to send e-mail. Packets are addressed to a specific port at a specific IP address.

Firewalls

A firewall separates one portion of a network from another and allows only authorized network traffic to pass through. On a small business network, a firewall typically separates the local private network from the Internet. Some firewalls examine the packets that flow in and possibly out of the network to make sure that they are legitimate; firewalls can also filter out suspicious packets. Firewalls hide the identities of computers within your private network to make it harder for criminal hackers to target individual computers (Figure 1).

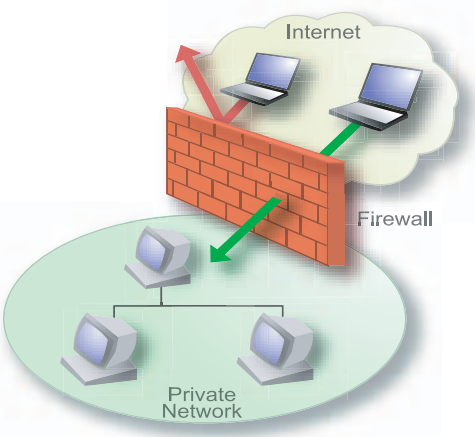

Figure 1. A firewall allows network traffic from valid users (the green line) to pass through to your network but blocks traffic from intruders (the red line).

Servers

A server is really just another computer attached to a network that is designated to perform some special function, such as share a printer, store files, or deliver Web pages. Remember that if your laptop or desktop computer is connected to the Internet, it is also a kind of server and, without a firewall, is capable of receiving unwanted traffic from the Internet.

Common Security Threats Against Networks

Attackers have different motivations—profit, mischievousness, glory—but they all work in similar ways. Several basic threats exist, all of which are capable of infinite variation.

Did You Know?

Each day, Microsoft filters out over three billion spam messages and protects the inboxes of over 200 million users worldwide.

Spam. Spam, or unsolicited commercial e-mail messages, wastes bandwidth and time. The sheer volume of it can be overwhelming, and it can be a vehicle for viruses. Much of it is of an explicit sexual nature, which in some cases can create an uncomfortable work environment and, potentially, legal liabilities if companies do not take steps to stop it.

Spoofing. A couple of kinds of spoofing exist. IP spoofing means creating packets that look as though they have come from a different IP address. This technique is used primarily in one-way attacks (such as denial of service, or DoS, attacks). If packets appear to come from a computer on the local network, it is possible for them to pass through firewall security (which is designed to protect against outside threats). IP spoofing attacks are difficult to detect and require the skill and means to monitor and analyze data packets. E-mail spoofing means forging an e-mail message so that the *From* address does not indicate the true address of the sender. For example, a round of hoax e-mail messages circulated the Internet in late 2003 that were made to look as though they carried a notice of official security updates from Microsoft by employing a fake Microsoft e-mail address. Dozens of industry leaders, including Microsoft, have co-developed a technology called the Sender ID Framework (SIDF) that helps to counter e-mail spoofing and phishing by validating that messages come from the mail servers they claim to come from.

Phishing. Phishing is increasingly becoming a tactic of choice for hackers and organized crime. Typically, an attacker sends an e-mail message that looks very much like it comes from an official source (such as eBay or Microsoft). Links in the message take you to a website that also looks like the real thing. However, the site is just a front, and the goal of the scam is to trick you into giving away personal information, sometimes for spam lists, sometimes so that the perpetrators can steal your account information or even your identity. The victims of these scams are not only the users who may divulge personal and confidential information, but also the spoofed business' brand and reputation.

Did You Know?

In June 2004, the Gartner Group reported that online bank accounts had been looted of $2.4 billion just in the previous 12 months. It estimated that 1.98 million adults had suffered losses. Much of the problem was traced to malicious programs that surreptitiously collect passwords and other confidential data. "Phishing" schemes also were used.

Viruses. Viruses are programs designed to replicate themselves and potentially cause harmful actions. They are often hidden inside innocuous programs. Viruses in e-mail messages often masquerade as games or pictures and use beguiling subjects (for example, "My girlfriend nude") to encourage users to open and run them. Viruses try to replicate themselves by infecting other programs on your computer.

Worms. Worms are like viruses in that they try to replicate themselves, but they are often able to do so by sending out e-mail messages themselves rather than simply infecting programs on a single computer.

Trojan horses. These malicious programs pretend to be benign applications. They don't replicate like viruses and worms but can still cause considerable harm. Often, viruses or worms are smuggled inside a Trojan horse.

Did You Know?

According to the National Cyber Security Alliance, 62 percent of computer users have not updated their antivirus software, and a staggering 91 percent in the study have spyware on their computers that can cause extremely slow performance, excessive pop-up ads, or hijacked home pages.

Spyware. Spyware refers to small, hidden programs that run on your computer and are used for everything from tracking your online activities to allowing intruders to monitor and access your computer. You might be the target of spyware or other unwanted software if you download music from file-sharing programs, free games from sites you don't trust, or other software from an unknown source.

Tampering. Tampering consists of altering the contents of packets as they travel over the Internet or altering data on computer disks after a network has been penetrated. For example, an attacker might place a tap on a network line to intercept packets as they leave your establishment. The attacker could eavesdrop or alter the information as it leaves your network.

Repudiation. Repudiation refers to a user's ability to falsely deny having performed an action that other parties cannot disprove. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit records) can prove otherwise.

Information disclosure. Information disclosure consists of the exposure of information to individuals who normally would not have access to it. For example, a user on your network might make certain files accessible over the network that should not be shared. Employees also tend to share important information, such as passwords, with people who should not have them.

Denial of Service. DoS attacks are computerized assaults launched by an attacker in an attempt to overload or halt a network service, such as a Web server or a file server. For example, an attack may cause a server to become so busy attempting to respond that it ignores legitimate requests for connections.

Elevation of privilege. Elevation of privilege is a process by which a user misleads a system into granting unauthorized rights, usually for the purpose of compromising or destroying the system. For example, an attacker might log on to a network by using a guest account, then exploit a weakness in the software that lets the attacker change the guest privileges to administrative privileges.

Pirated software. The use of counterfeit software is widespread. In some parts of Asia and the former Soviet Union, at least 90 percent of the software used is counterfeit. Even in the United States, an estimated 25 percent of software is counterfeit. While the low prices of counterfeit software can be attractive, such software comes with a potentially much higher price: Counterfeit software can contain bugs and viruses and is illegal. Genuine Microsoft software provides up-to-date protection against hackers and e-mail viruses, plus improved system recovery tools. You can learn more about genuine Microsoft software by visiting www.microsoft.com/genuine/small_business.px?displaylang=en

Did You Know?

Earthlink, the Atlanta-based Internet Service Provider, said in April 2004 that it had found 370,000 Trojan horses and system monitors on the 1.6 million computers it had studied. If Earthlink's numbers hold up for all computers, up to 35 percent are compromised.

Most attackers use the processing power of computers as their weapon. They might use a virus to spread a DoS program to thousands of computers. They might use a password-guessing program to try every word in the dictionary as a password. Of course, the first passwords they check are "password," "letmein," "opensesame," and a password that is the same as the username.

Attackers have programs that randomly probe every IP address on the Internet looking for unprotected systems and, when they find one, have port scanners to see whether any ports are open for attack. If these attackers find an open port, they have a library of known vulnerabilities they can use to try to gain access. For more deliberate attacks, such as industrial

espionage, a combination of technology and social engineering is most effective. For example, inducing members of your staff to reveal confidential information, rifling through trash in search of revealing information, or simply looking for passwords written on notes by monitors are all options.

Why Software Is Vulnerable

Software developers do not set out to write unsafe programs. For example, a typical operating system is the product of tens of thousands of hours of work and consists of millions of lines of code. A simple bug or oversight can provide an unexpected backdoor into an otherwise secure system. It is impossible to write bug-free software. Of course, that doesn't mean developers should give up trying to do so.

Then there are the bad guys. Bank robber Willie Sutton once said, "I rob banks because that's where the money is." It's the same with software. The more successful and widespread a piece of software is, the more likely attackers are to target it. There is a continual struggle between attackers exploiting weaknesses and developers seeking to eliminate those weaknesses. It's the same with locksmiths and burglars, and with alarm manufacturers and car thieves. This is why software developers release updates that fix known vulnerabilities and why you should install those updates. (For information about securing computers, see the section, "Microsoft Windows XP Service Pack 2.")

The Importance of Software Updates

According to the Symantec Internet Security Threat Report published in September 2004, it takes on average 5.8 days after a software vendor announces a vulnerability for criminal hackers to take advantage of the discovery. You should apply software updates as soon as possible when they are announced. You should use the Automatic Updates feature in Microsoft Windows XP to download and install updates automatically and also make sure that your antivirus software is updated regularly. Consider signing up for Microsoft Security Update e-mail bulletins, a free service you can learn more about at www.microsoft.com/security/bulletins/alerts.mspx

Finding the Right Consultant

Most small businesses do not have dedicated technology staff. Hiring a consultant can help you determine the security solution that is right for your business. Finding the right consultant can be trying, but good support makes technology easier to manage and ensures that you get the best possible advice and implementation.

Where Do You Start?

Ask your colleagues, suppliers, and peers whom they use. Ask your local Chamber of Commerce or SBDC for their input.

What Are You Looking For?

If you are not already working with a partner, look for someone who can help you now and in the long term. Look for evidence of the ability to grow and develop as a company and support businesses bigger than yours. The following checklists can help you select the right company.

Experience

- Does the consulting group have a Certified Information Systems Security Professional (CISSP) engineer on staff? If they have a CISSP on staff, you should feel good about the consultant's level of security expertise.
- Do they have a CompTIA Security+ Certification? CompTIA Security+ measures industry-standard knowledge and competencies for managing information security.

- Does the consulting group have a Microsoft Certified System Engineer (MCSE) or Microsoft Certified Systems Administrator (MCSA) on staff? MCSEs are specialized in understanding how to design, implement, and administer security for a Microsoft Windows Server™ 2003-based network. MCSAs specialize in understanding how to administer network environments.
- How long has the consulting group been in business and how many customers do they have? Are they willing to provide a list of customers you can talk to about the group's services?

Services

- Which of the following security services does the consulting group provide?

  a) Antivirus installation and support
  b) Hardening servers (i.e., ensuring that all system settings are at the appropriate level of security)
  c) Hardening desktop computers
  d) Firewall installation, configuration, and support
  e) Intrusion detection

- Do they provide security audits? On which operating systems?
- Do they provide 24×7 remote or on-site security support?
- What levels of support will they provide? Look for a service level agreement that sets out how quickly they will respond to problems and the level of after-sales support they offer.
- Can they provide or recommend reputable trainers?

- Will they be able to grow with you in the future?

Approach

- Does the consultant apply consistent patterns and practices in its operations? Ask to see an outline of its process.
- Can they commit to a specific schedule and budget for a given project?
- Will they be able to do the work with their own staff, or will they have to subcontract?
- What is their fee structure? Depending on the project, it is possible to agree on a flat fee, an hourly or daily rate, or an ongoing retainer. Are they willing to break down their cost structure and allocate costs to different stages or activities? You want accurate, exact, and precise information before any work is commissioned.
- How do they approach documentation? They should supply you with a proposal for the work, including a budget, a timetable, and a reasonable specification. The proposal should be in plain English.
- If their proposal is satisfactory, you should have a written contract specifying what is going to be done and by whom. Make sure to include dates, deadlines, equipment, costs, and so on. Even if you do not have a formal contract drawn up by attorneys, make sure that the details of the work are written down and agreed to in some form.

Where To Go Next

To find a Microsoft Small Business Partner, use these steps:

1. Visit the Microsoft Small Business Partner Finder website: www.microsoft.com/smallbusiness/partner/vendorsearch.mspx
2. Enter your zip code and desired proximity.
3. Check out those partners who offer security solutions.

10 Questions to Help Protect Your Business

Take our security quiz and find out how much you know—or don't know—about important security issues that can have an impact on your business.

1. Which of the following actions will **not** help you to secure desktop computers?
   a. Turn on Automatic Updates
   b. Turn on Windows Firewall
   c. Install antivirus software
   d. Open e-mail attachments from an unknown sender

2. Which of the following is an example of a strong password?
   a. Password
   b. J*p2le04>F
   c. My dog has fleas!
   d. Your real name, username, or company name

3. True or false: If you have a perimeter firewall on your network, you don't need to turn on Windows Firewall.
   a. True
   b. False

4. How can you prevent intruders from accessing your wireless network?
   a. Encrypt network traffic with Wi-Fi Protected Access (WPA) or Wired Equivalent Privacy (WEP)
   b. Restrict access to trusted Media Access Control (MAC) addresses
   c. Both

5. True or false: If you set antivirus software for auto-updates, you don't need to enable Windows Automatic Updates.
   a. True
   b. False

6. True or false: Small businesses are not targets for hackers.
   a. True
   b. False

7. What is phishing?
   a. "Spoofed" e-mail messages and websites that fool recipients into divulging personal information
   b. A type of computer virus
   c. An example of a strong password
   d. None of the above

8. What product can you use to update all the computers on your network?
   a. Windows Update Services (WUS)
   b. Microsoft Internet Information Services (IIS)
   c. Bluetooth Networking
   d. Microsoft Baseline Security Analyzer (MBSA)

9. What method(s) can you use to protect sensitive data from prying eyes?
   a. Passwords
   b. File permissions
   c. Encryption
   d. All of the above

10. How often should you perform an incremental backup?
    a. Daily
    b. Every other day
    c. Weekly
    d. Monthly

Answers to the security quiz appear below. If you didn't answer all the questions correctly, refer to the section "Seven Steps to Better Security" to learn more about security issues that concern small businesses.

1. **d.** You should use Automatic Updates, antivirus software, and Windows Firewall. You should never open e-mail attachments from an unknown source.
2. **b and c.** A strong password has a mixture of different character types. Passphrases make very secure passwords.
3. **b. False.** You should use a perimeter firewall and a local firewall, like Windows Firewall.
4. **c. Both.** You should encrypt your network and limit access.
5. **b. False.** Automatically updating your antivirus software does not also automatically update the Windows operating system. You should also enable the Windows Automatic Updates feature.
6. **b. False.** Small businesses are often direct targets of attacks and can also be affected by attacks on larger companies.
7. **a.** Spoofed e-mail messages and fraudulent websites are designed to fool recipients into divulging personal financial data, such as credit card numbers, account usernames, and passwords.
8. **a. WUS.** WUS provides a solution to the problem of managing and distributing critical Windows updates that resolve known security vulnerabilities and other stability issues in the Windows operating systems.
9. **d. All of the above.** You can protect sensitive data by using strong passwords, assigning file permissions, and enabling encryption.
10. **a. Daily.** An incremental backup includes all data that has changed since the last backup. You should perform an incremental backup daily if you are using this method as part of your backup solution.

Microsoft Windows XP Service Pack 2

Microsoft Windows XP Service Pack 2 (SP2) is a free upgrade for computers running Windows XP that includes every security update Microsoft has issued for this operating system and provides several significant security enhancements.

As part of a major effort to increase the security of desktop computers, Microsoft has released an update to Windows XP named Windows XP SP2. As with all Windows service packs, SP2 includes the critical updates released for Windows XP to date. SP2 also includes a large number of new enhancements to Windows XP—enhancements aimed at increasing the default level of security for your operating system.

Small Business Spotlight: W&E Baum:

"The installation of Windows XP Service Pack 2 (SP2) was fast and easy. When we rolled out Windows XP Service Pack 1, it took about 30 minutes, or $75 per computer. The SP2 rollout required just 5 minutes per computer, reducing our implementation costs by about 95 percent."

Automatic Updates

An important part of helping to keep Windows XP secure is keeping it up to date with the latest software updates that Microsoft has released. Automatic Updates can locate critical and security updates, download them, and install them automatically. SP2 provides several enhancements to the Automatic Updates feature in Windows XP, including the ability to download more categories of updates, better bandwidth management, and consolidation of updates so that less user input is required.

Windows Firewall

In the original release of Windows XP, the software-based firewall included with the operating system was named Internet Connection Firewall. With the release of SP2, this firewall has been renamed Windows Firewall and adds several new features. The updates include enabling Windows Firewall by default on all network connections, improving the user interface,

improving application compatibility when Windows Firewall is on, and providing a way to configure global settings for all network connections.

Internet Explorer

Security enhancements to Microsoft Internet Explorer provide improved protection against malicious content on the Web and also provide interface enhancements that make configuring security easier. A new Information Bar consolidates many of the dialog boxes Internet Explorer uses to provide information to users. Internet Explorer now includes a built-in pop-up window blocker as well as a feature called Manage Add-ons that lets you disable the scripting capabilities that allow rogue sites to hijack Internet Explorer and force you to go to their sites.

Outlook Express

SP2 also provides security enhancements for users of the Microsoft Outlook® Express e-mail program. You can block external content from being automatically downloaded and displayed in HTML-formatted messages and even configure Outlook Express to display messages only in plain text format. You can also block potentially unsafe attachments that are sent through e-mail messages, and instant messages are isolated so that they cannot affect other parts of the system.

Wireless Support

A new interface in SP2 makes it easier to find a wireless network by telling you what networks are available, their strength, and their type of security. You can easily move between networks, if necessary. The Wireless Network Setup Wizard makes establishing a wireless network virtually painless. Furthermore, new wizards step you through configuring security features for your wireless network, whether you use the old WEP or the new, much stronger, WPA.

Security Center

Security Center is a new feature that provides a central interface showing the status of security configurations on a computer, including settings for Automatic Updates, Windows Firewall, and some non-Microsoft antivirus software. Security Center also runs as a background service and provides real-time alerts when certain security conditions are detected. Armed with the enhanced security technologies that SP2 provides, you will experience a more secure desktop environment than ever before. For more information and to find out how you can get Windows XP SP2 at no cost, visit www.microsoft.com/windowsxp/sp2/default.mspx

This section outlines the basic security measures that every company should take to help protect itself. Refer to the section "What You Need to Know About Security" for information about anything that seems too technical, or speak with an information technology (IT) or security consultant. These steps assume that you have a security policy and security plan in place. For an example of a security policy and security plan, see the section "Sample Security Plan: Adventure Works."

Step 1 Protect Your Desktops and Laptops

If you take only three precautions to help safeguard the computers you use in your business, make them the following:

- Update your software.
- Help protect against viruses.
- Set up firewalls.

Taking these actions won't keep you completely safe from security threats and productivity loss, but together they give you a powerful first line of defense.

Update Your Software

Criminal hackers like to find and exploit bugs and loopholes in popular software products. Some do it for money, some to make a statement, and some simply to cause trouble. And they can cause trouble—exposing customer credit card numbers on a website or stealing passwords in a computer. The impact on a business can be fatal.

Basic steps you can take

When Microsoft or any other software company discovers a vulnerability in its software, it typically releases an update that can be downloaded over the Internet. The update "patches" the loophole or bug to keep hackers from causing trouble. Over time,

however, software products have become more secure. For example, Microsoft Windows XP Professional is inherently more secure than Microsoft Windows 95. Windows XP Professional with SP2 provides even stronger security settings that help defend against hackers, viruses, and worms. But that doesn't negate the importance of downloading and installing appropriate updates as soon as they are released.

Manually install updates for Windows

- **Windows XP Professional:** Go to the Windows Update website (http://windowsupdate.microsoft.com), and then click Scan for Updates. The website automatically analyzes your computer, determines which updates you need, and then makes them available for download. To make the update process easier, enable the Automatic Updates feature. With this feature, Windows XP Professional can monitor for, download, and install updates automatically (depending on the settings you select).

- **Windows 2000:** If you're running Microsoft Windows 2000 as part of a domain or as a standalone computer, visit the Windows Update website (http://windowsupdate.microsoft.com), where you will find the latest service packs, device drivers, application-compatibility information, and system security updates. In a domain environment, server computers running Microsoft Windows 2000 Server or Windows Server 2003 manage the security for all resources on the network.

What Version of Windows Do I Have?

If you are unsure which version of Windows you are running, it's easy to find out. Microsoft provides an online tool that can determine your version of Windows (including any Service Packs installed). Just use these steps:

1. Go to **www.microsoft.com/protect/**
2. Click the *"Find out which version of Windows your computer is using"* link at the bottom of the page.

You can also determine your Windows version manually (and without going online) by using the following steps:

1. Click Start, and then click Run.
2. In the Run dialog box, type winver, and then click OK.
3. In the About Windows dialog box that appears, look for the installed version of Windows and any Service Packs that are installed.

- **Windows Me, Windows 98, Windows NT®, and Windows 95:** Older versions of Windows, such as Microsoft Windows Me or Windows 98, are much less secure than newer versions. Microsoft strongly encourages upgrading to newer versions of Windows to ensure the highest level of security.

Automatically download and install updates on a computer running Windows XP Professional

1. Click **Start,** and then click **Control Panel.**
2. In Control Panel, double-click **System**.
3. In the System Properties dialog box, click the **Automatic Updates** tab (Figure 2).
4. Select the **Automatic (recommended)** option.
5. From the drop-down lists, select the day and time each day to download and install updates.
6. Click **Apply**, and then click **OK**.

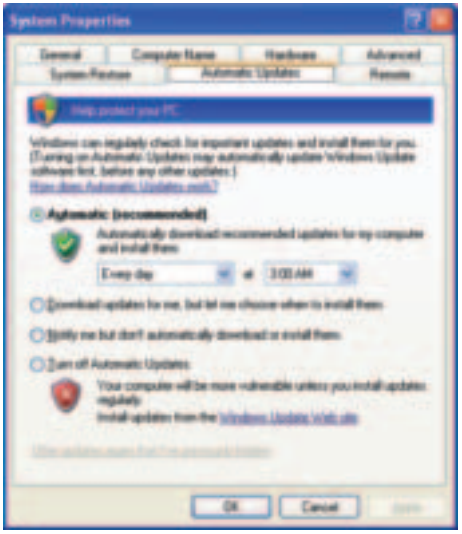

Figure 2. Set up your computer to download and install updates automatically.

You can also keep current with security updates for Microsoft Office. These updates and other downloadable add-ins are available by going to the Office Update website (http://office.microsoft.com) and clicking **Check for Updates.**

Help Protect Against Viruses

Viruses, as well as worms and Trojan horses, are malicious programs that run on your computer. Some viruses delete or change files. Others consume computer

resources. Some allow outsiders access to your files. Viruses can replicate, or copy, themselves, even send themselves to e-mail addresses in a contacts list. Virus-infected computers can spread the virus throughout your company and cause serious downtime and data loss. You also risk infecting the computers of clients and customers you communicate with via e-mail.

Basic steps you can take

You should have antivirus protection on all your computers. Antivirus software works by scanning the contents of incoming e-mail messages (and files already on your computer) to detect virus signatures. If the software finds a virus, the software deletes or quarantines it.

Did You Know?

A survey conducted by America Online found that 20 percent of home computers were infected by a virus or worm and that various forms of snooping programs are on 80 percent of computers. Despite that, more than two-thirds of home users think they are safe from online threats.

Install antivirus software

Because hundreds of viruses are released each month, all antivirus software must be updated regularly with the latest signature definitions so that the software can catch the latest viruses. Look for software that automatically downloads the latest definitions and programs from the Internet. (If your company uses laptop computers, see the sidebar "Taking Special Care of Laptop Computers" on page 26.) Here are links to antivirus programs from some of the better-known security software makers:

- AVG Anti-Virus: www.grisoft.com/
- Norton AntiVirus: www.symantec.com/smallbiz/nav/
- McAfee VirusScan: www.mcafee.com/
- Panda Titanium Antivirus: www.pandasoftware.com/
- BitDefender: www.bitdefender.com/
- Microsoft Malicious Software Removal Tool: visit www.microsoft.com/downloads/ and type "Malicious Software Removal Tool" into the **Search** box

Never open suspicious files

Make sure everyone in your company understands that they should delete—without opening—any e-mail attachments from an unknown, suspicious, or untrustworthy source.

Help Protect Your Inbox

Microsoft has developed SmartScreen™ technologies that are integrated into many Microsoft products, including MSN® Hotmail, Microsoft Exchange Server, and Microsoft Office Outlook® 2003. These products have settings that help detect and eliminate unwanted e-mail. Look into upgrading to these programs if you don't use them already.

To set junk e-mail options in Office Outlook 2003, use these steps:

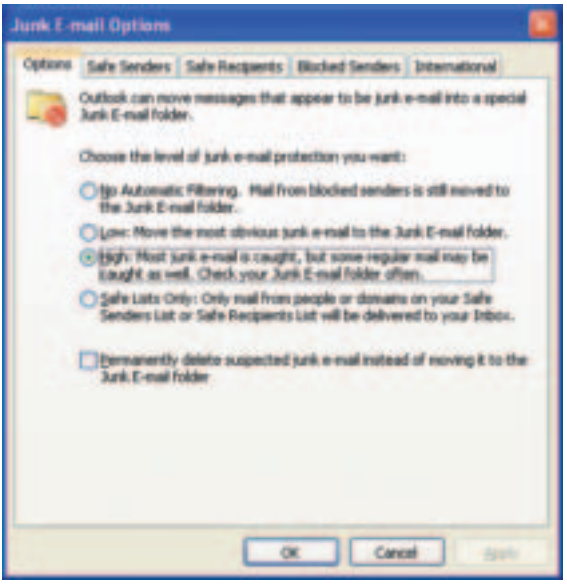

Figure 3. Enable junk e-mail filtering in Office Outlook 2003.

1. In Office Outlook 2003, click the **Actions** menu.
2. Select **Junk E-mail**, and then click **Junk E-Mail Options.**
3. On the Junk E-mail Options dialog box, select the level of junk e-mail protection you want from the list of choices (Figure 3).
4. Click **Apply,** and then click **OK**.

Office Outlook 2003 makes available (free of charge) monthly updates to its junk e-mail filter. Users are advised to download these updates routinely to help counter new deceptive e-mail tactics. To learn more about the security and spam-blocking features in Office Outlook 2003, visit the Office Outlook 2003 Web page:
www.microsoft.com/office/editions/prodinfo/junkmail.mspx

For Junk Mail Filter updates, visit
http://office.microsoft.com/en-us/officeupdate/ and click **Downloads for Office 2003.**

To upgrade to Outlook Express 6.0, download and install Internet Explorer 6.0 from the Office 2003 Downloads Web page:
www.microsoft.com/windows/ie/enthusiast/videos/email.mspx

To learn more about viruses, read the article *"7 things to know about virus writers"* at www.microsoft.com/smallbusiness/issues/technology/security/7_things_to_know_about_virus_writers.mspx

Set Up Firewalls

If you have an always-on broadband connection, chances are that your company's computer network is randomly probed by criminal hackers. When intruders stumble on a valid computer address, they try to exploit vulnerabilities in software to gain access to your network—and ultimately individual machines.

Basic steps you can take

Like a moat around a castle, a firewall can block intruders from gaining access to your private network. There are two basic types of firewalls:

- **Perimeter firewalls.** These firewalls block all traffic between the Internet and your network that isn't explicitly allowed. For example, you may want to configure the firewall to accept certain kinds of e-mail and Web traffic but reject all

other types of traffic. Firewalls can also hide the addresses of the computers behind your firewall, making individual computers on your network invisible to the outside. A firewall may be integrated into a router or DSL/cable modem or a software product like Microsoft Internet Security and Acceleration (ISA) Server.

- **Local firewalls.** Local firewalls must be installed on each computer. The Windows Firewall in Windows XP SP2 is enabled by default, which means that, by default, all the connections—including LAN (wired and wireless), dial-up, and Virtual Private Network (VPN) connections—are protected.

Taking Special Care of Laptop Computers

Laptop computers are a tempting target because they are easy to steal and to sell. Think of it as leaving a pile of cash equal to the cost of the laptop just lying around. Besides the hassle and cost of replacement, there is the risk that a stolen laptop computer contains hard-to-replace or confidential information. If you use a laptop computer, consider these special precautions:

- Use a strong password. Make sure you shut down the laptop computer when it is unattended.
- Keep the laptop computer within sight, particularly in crowded public areas like train stations and airport security checkpoints, but also at meetings and conferences.
- Keep your laptop computer in your carry-on luggage, and don't leave it in hotel baggage-hold rooms. Don't carry laptop computers in cases stamped with a manufacturer's logo or in cases that look too much like a laptop case.
- Keep a record of your laptop computer's serial number and all the software or accessories you use.
- Back up all the work stored on your laptop computer before a trip and, if possible, continue to make backups of work you do on the road. Sending new documents home by e-mail is one way to do this.
- Use the Encrypting File System (EFS) to secure confidential files. For advice on this process, see Microsoft support article 223316, "Best Practices for the Encrypting File System," at: http://support.microsoft.com/default.aspx?scid=kb;EN-US;223316

If your computers are not running Windows XP, you can purchase a commercial local firewall. The following software vendors sell commercial firewall software:

- ZoneLabs (www.zonelabs.com)
- McAfee (www.mcafee.com)
- Symantec (www.symantec.com)

Read More About It

- For articles from Microsoft about securing desktop and laptop computers, visit the Microsoft Security website: www.microsoft.com/smallbusiness/gtm/securityguidance/checklist/default.mspx
- If you are not using Windows XP Professional with SP2, you can find information on alternative software-based local firewalls at www.mcafee.com, www.symantec.com, or www.zonelabs.com
- For information about the different types of firewalls available and for technical details about how firewalls work, read the information on Microsoft TechNet at www.microsoft.com/technet/security/topics/network/firewall.mspx
- For information about spyware, visit www.microsoft.com/athome/security/spyware/default.mspx
- For an excellent introduction to the world of criminal hackers, including interviews and useful background reading, visit www.pbs.org/wgbh/pages/frontline/shows/hackers/

Step 2 Keep Your Data Safe

Implementing a regular backup procedure is a simple way to help safeguard critical business data. Setting permissions and using encryption will also help. Much of the misfortune that small businesses experience can be blamed on outside

forces—a poor economy, a natural disaster, a decision by a key employee to leave. It's no surprise that those who survive the down times are typically those who minimized their risks by taking basic precautions. One of the most basic precautions of all is protecting critical business data.

Just imagine walking into your office one morning and discovering that all your sales records, customer contact information, and order history had disappeared. How long would it take you to recover? How much disruption and delay would occur? What would it cost you?

Data loss can and does happen. It can result from hardware failure, flood, fire, security breach, or just an accidental deletion of an important file. Whatever the cause, taking precautions to reduce the impact is like an insurance policy, enabling your business to get back up and running quickly.

Basic Steps You Can Take

There are numerous ways to help safeguard your critical business data, but these three methods will get you started.

Implement a procedure to back up critical data

Backing up data means making a copy of it on another medium. For example, you might burn all your important files onto a CD-ROM, a second hard drive, or a shared folder on your network. There are two basic kinds of backups: a full backup and an incremental backup. A full backup makes a complete copy of the selected data onto another medium. An incremental backup backs up just the data that has been added or changed since the last full backup. You should also keep copies of backups at a secure offsite location.

A full backup augmented by incremental backups is generally quicker and takes less storage space. You might consider a policy of running a full backup on a weekly basis, followed by daily incremental backups. However, when you want to restore

data after a crash, this method will take longer because you first have to restore the full backup, then each incremental backup. If such a process is a concern, another option is to run a full backup nightly; just automate it to run after-hours (Figure 4).

Test your backups frequently by actually restoring data to a test location. In this way, you can:

- Ensure backup media and backed-up data are in good shape.
- Identify problems in the restoration process.
- Provide a level of confidence that will be useful during an actual crisis.

Establish permissions

Both your desktop and server operating systems can provide protection against data loss resulting from employee activities.

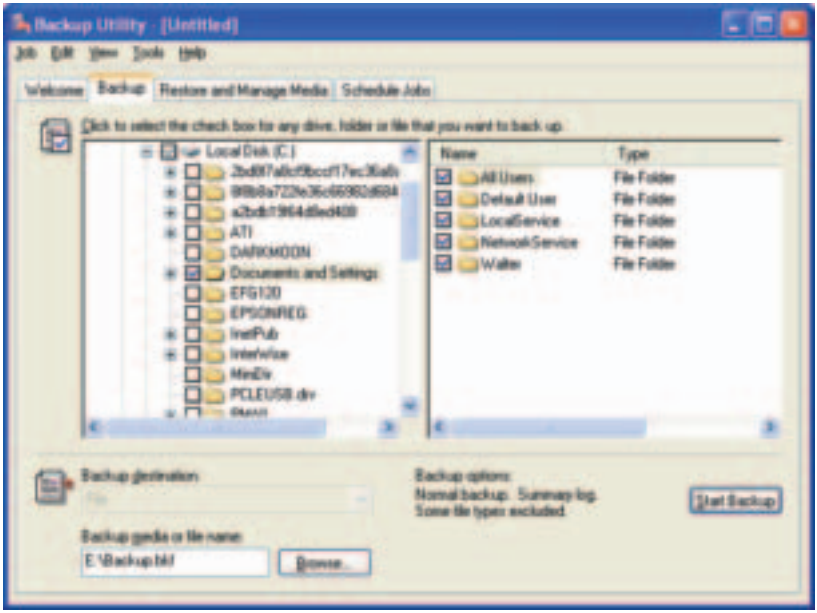

Figure 4. Back up critical data and test the backups by restoring them.

With Windows XP and Windows 2000—as well as Microsoft Windows Small Business Server (SBS) 2003, Windows Server 2003, and Windows 2000 Server—it is possible to assign users different permission levels based on their roles and responsibilities within your organization. Rather than giving all users Administrator access—which is not a best practice for maintaining a secure environment—institute a "least privilege" policy by configuring your servers to give individual users access to specific programs only and specifically defining user privileges.

Encrypt sensitive data

Encrypting data means that you convert it into a form that disguises the data. Encryption is used to ensure the confidentiality and integrity of the data when the data is stored or moved across a network. Only authorized users who have the tools to decrypt encrypted files can access these files. Encryption complements other access control methods and provides an added level of protection for securing data on computers that may be vulnerable to theft, such as mobile computers or files shared on a network. Windows XP and Small Business Server 2003 support Encrypting File System (EFS) to encrypt files and folders. Together, these three practices should provide the level of protection most businesses require to keep their data safe.

Why You Should Test Your Backups

Erik was the managing director of a growing architectural firm. With 30 employees and several multinational clients, the company relied on its e-mail system to keep in touch and to track client requests. Then, one afternoon, the e-mail server had a catastrophic hardware failure, and the data became corrupted.

"No problem," thought Erik, "our support guy has a backup, so we can just restore it from that." In fact, the company had an elaborate tape library and dutifully kept offsite copies of its critical backups. It was only after a day's work of trying to restore the e-mail system from the backup tapes that they realized the data hadn't been properly backed up. They had never noticed the problem and had never tested to see whether restoring the data worked properly. They did not have any kind of disaster recovery plan in place.

Read More About It

- For articles from Microsoft about keeping data safe, visit www.microsoft.com/smallbusiness/gtm/securityguidance/checklist/default.mspx
- For more information about how to use Microsoft Backup, go to www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp

Step 3 Use the Internet Safely

Unscrupulous websites, as well as pop-ups and animations, can be dangerous. Set rules about Internet usage to protect your business—and your employees.

If your business doesn't have a policy on Internet use, it should. Though the Web can be an incredibly useful workplace tool, it can also cause significant workplace havoc that can result in lost productivity. Setting some rules protects your business and your employees.

Why Your Business Is at Risk

Web pages contain programs that are usually innocent and sometimes helpful—for instance, animations and pop-up menus. But there are questionable, even malicious websites that have their own agenda, and it's not always in your best interest to browse them. When you're surfing the Web, site operators can identify your computer on the Internet, tell which page you came from, use cookies to profile you, and install spyware on your computer—all without your knowledge. Destructive worms can also enter your system through your Web browser.

Beyond malicious activities instigated by outsiders, businesses can be put in a vulnerable position by employees who engage in illegal or undesirable Web activity during work hours and on company-owned computers.

What Your Internet Policy Should Include

When creating a company-wide Internet-use policy, address the following issues:

- Whether employees are allowed to browse the Web for personal use as well as business purposes
- When employees can use the Web for personal use (for example, lunch hours, after hours)
- If and how the company monitors Web use and what level of privacy employees can expect
- Web activity that is not allowed. Spell out unacceptable behavior in detail. In many companies this behavior includes activities such as:
  - **Offensive content downloads**
  - **Threatening or violent behavior**
  - **Commercial solicitations (non-business related)**
  - **Other illegal activities**

Provide two copies of the policy to employees—one for them to keep and another for them to sign and return to you. (For more information, see the section "Creating a Security Policy," later in this guide.)

Tips for Safe Browsing

In addition to having a policy, the following recommendations can also help promote safe Web browsing:

- Go to trusted sites only.
- Don't use work computers for idle browsing.
- Never browse websites from a server. Always use a desktop or laptop computer.
- Do not allow websites to install programs unless you trust the website and are sure of what the program does.
- Use a firewall or a router. Doing so allows you to filter Web addresses and block Internet traffic to and from dangerous sites.
- Consider Web-filtering software. Companies such as Websense and Secure Computing offer products that filter Internet use based on a variety of criteria.

Read More About It

- For articles from Microsoft about using the Internet safely, visit www.microsoft.com/smallbusiness/gtm/security guidance/checklist/default.mspx
- For Web-filtering software, visit www.microsoft.com/spam, www.microsoft.com/windowsserver2003/sbs/default.mspx, www.securecomputing.com and www.websense.com
- To research possible hoaxes, visit www.symantec.com/avcenter/hoax.html
- For more information about combating spyware, visit www.microsoft.com/spyware/
- To implement the Sender ID Framework to protect your domain name from e-mail forgery, visit www.microsoft.com/senderid/

Step 4 Protect Your Network

Remote access to your network may be a business necessity, but it is also a security risk you need to monitor closely. Use strong passwords and be especially cautious about wireless networks.

Nobody likes to think the worst—that around every corner someone is snooping into your business affairs. But if your company operates either a wired or wireless network and has information that you would like to keep confidential, a little paranoia will serve you well.

Basic Steps You Can Take

Here are four basic measures that can help reduce your network security fears.

Set up firewalls

A firewall controls access to and from your network or

computer, blocking intruders from accessing your private network and controlling what your employees can access outside your network. Perimeter firewalls protect all the computers on your network. They also offer an additional layer of defense because they can effectively make all your network computers "invisible" to the outside world.

Use strong passwords

Most small businesses use passwords to authenticate identity, whether on computers, cash registers, or alarm systems. Although more sophisticated authentication systems exist, such as smart cards and fingerprint or iris scans, passwords are most common because they are easy to use. Unfortunately, they are also easily misused. Hackers have automated tools that help them crack simple passwords in minutes. Crooks may also use fraud to get employees to divulge passwords.

Too often, passwords are not effective for these reasons:

- Sensitive documents have not been password-protected, allowing anyone to walk up to an unsecured computer and log on.
- Passwords are weak or are never changed.
- Passwords are written down in plain sight.

Did You Know?

According to studies at Michigan State University and elsewhere, up to 70 percent of identity thefts are conducted by insiders or people posing as insiders. Strong passwords help protect against this kind of threat.

Educating your staff about the importance of passwords is the first step in making passwords a valuable network security tool. Employees should regard their passwords the same way they would an office key. In other words, don't leave it lying around and don't share it. Employees should also **avoid** weak and easy-to-guess passwords that include the following:

- Their real name, username, or company name
- A common dictionary word that makes them vulnerable to "dictionary attacks," in which a program attempts to use words found in a dictionary to log on to a system
- Common passwords, such as "password," "letmein," or "1234"
- Commonly known letter substitutions, such as replacing "i" with "!" or "s" with "$"
- A password that someone else knows
- Using no password at all, which makes it easy for other employees to just walk up to an unsecured computer and log on
- Any password that they write down

What does a strong password look like? It should have the following characteristics:

- Be at least eight characters long (the longer, the better)
- Have a combination of lowercase and uppercase letters, numbers, and symbols
- Be changed at least every 90 days and, when changed, should be significantly different from previous passwords

Of course, a password you can't remember is no use at all. There are some tricks that can make strong passwords more memorable:

- In Windows 2000 and Windows XP, you can use a passphrase such as "I had 5 chicken tacos for lunch."
- You could also pick a phrase, then use only the first character of every word, such as Msi5Yold! (My Son is 5 years old!).
- Another trick is to take short, simple words and join them together with numbers and symbols (for example, Tree+34+Pond).

Use wireless security features

Wireless networks use a radio link instead of cables to connect computers. As a result, anyone within radio range can theoretically listen in or transmit data on the network. Freely available tools allow intruders to "sniff" for insecure networks. While vulnerability increases with a wireless network, computer-savvy crooks have tools to help them break into all types of computer systems.

Security features are built into Wi-Fi products, but manufacturers often turn the features off by default to make network setup easier. If you use wireless networking, make sure you turn the security features on and use the security and access features that will make your network more secure.

Also consider these tips:

- Restrict wireless access (if your wireless network provides this feature) to office hours or whenever you expect to use the network.
- Filter out casual intruders by setting access points to restrict network access to specific computers.
- Use the encryption built into your wireless access point to encode information as it travels across the network and prevent any non-authorized party from reading or changing data.

War Driving

Anyone with a laptop computer, an inexpensive wireless network card, freely downloaded software, and an antenna made from something as simple as a can of potato chips can hack into wireless networks.

Most wireless networks are completely unsecured. Indeed, many manufacturers of wireless devices leave encryption turned off by default. Users tend not to enable wireless encryption or use any other added security measures, making it a relatively easy task for anyone with a wireless setup to find and exploit the connection. War driving is more than a geek prank. Some intruders seek to access files and damage systems. Fortunately, securing a wireless network is relatively easy, and the majority of war drivers can be deterred or deflected by a few simple steps.

Close unnecessary network ports

Network traffic for various applications are identified using numbered ports. In order for an application's traffic to get through a firewall, the firewall must allow traffic on that port. To strengthen your network's security against unauthorized access, close unused or unnecessary ports by using perimeter firewalls, local firewalls, or Internet Protocol Security (IPSec) filters. But a word of caution: Microsoft server products use a variety of numbered network ports and protocols to communicate with client and server systems. Blocking ports that the Microsoft Windows Server System™ uses may prevent a server from responding to legitimate client requests, which could mean the server won't function properly, if at all.

Read More About It

- For articles from Microsoft about protecting your network, visit www.microsoft.com/smallbusiness/gtm/securityguidance/checklist/default.mspx
- To configure a password policy in Windows Server 2003 (or Small Business Server 2003), go to www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/password_grouppolicy.asp
- For information about mobilizing your business, visit www.microsoft.com/smallbusiness/gtm/mobilize/hub.mspx

Step 5 Protect Your Servers

If you think of your servers as your network's command center, it's easy to understand why keeping them safe from attack is mission-critical. When your servers are compromised, your entire network is at risk. While some server attacks are merely annoying, others can cause serious damage.

If you have a small business, you may not have more than one or two servers. But no matter how few or how many servers

your business is running, your network relies on them. They serve the applications, Web pages, or e-mail that your team needs to do their jobs. They store valuable and confidential information resources. They provide a means for your customers to communicate with you, perhaps even purchase goods or services from you.

So, if your servers are down, you lose productivity, you jeopardize customer relationships, and you may even take an economic hit.

Basic Steps You Can Take

Many of the procedures already discussed will help protect your servers, too. If you haven't yet taken the steps already outlined in this guide, make them a priority. Even if you have already addressed the security measures discussed to this point, you can do still more to protect your servers.

Keep your servers in a safe place

Businesses must make sure that their servers are not vulnerable to physical calamities. Locate these machines in a locked, well-ventilated room, not in a hallway or under a desk. Servers should never be used as workstations. Your server room should have no windows and a single door you can lock. Server cases should also be locked to prevent tampering with internal components. Know which employees have keys to the server room. You should also keep a record of the serial numbers of your servers and mark the machines with your company information so that they can be identified and recovered if stolen.

Practice least privilege

The principle of least privilege dictates that users should be given only the permissions they need to do their jobs, but no more permissions than that. With Windows 2000 Server, Windows Server 2003, and Small Business Server 2003, it is possible to assign users different permission levels to local and

network resources. Rather than giving all users Administrator access—which is not a best practice for maintaining a secure environment for workstations or servers—you should use your servers to manage client computers. Windows servers can be configured to give individual users access to specific programs only and to define which user privileges are allowed on the server. In this way, you ensure that users can't make changes in areas that are critical to server or workstation operation. It also prevents users from installing software that may introduce a virus or spyware to their computers, which in turn can compromise the integrity of your entire network.

Understand your security options

Today's server operating systems are more secure than ever, but the powerful security settings you find in Windows Server System products are good only if they are used appropriately and monitored aggressively. If your team doesn't have an IT specialist or expertise in security issues, consider hiring an outside consultant to help appropriately protect your servers.

Read More About It

- For articles about protecting your servers, visit the Security Guidance Center for Small Business at www.microsoft.com/smallbusiness/gtm/securityguidance/hub.mspx
- For information about Windows Server 2003 or Small Business Server 2003, visit www.microsoft.com/server/ You can also find information about using servers on your network in the Networking Basics for Small Businesses guide, available at www.microsoft.com/smallbusiness/gtm/encomm/freetrial.mspx

Step 6 Secure Line-of-Business Applications

Make sure that software critical to your business operations is fully secure. Internal and external vulnerabilities can lead to lost productivity—or worse. Many companies rely on specialized business programs for accounting tasks, running point-of-sale systems, tracking inventory, and managing supply chains. These programs—sometimes dubbed line-of-business (LOB) applications—typically run on a server and operate in conjunction with a database. This integrated setup offers great advantages. Multiple employees can work with an LOB program and access the database information—all at the same time.

Understand Your Business Requirements

No matter what kind of business you operate, it is important for you to take the security precautions covered in this guide. In some businesses, however, government regulations, insurance policies, and special agreements require that you take extra precautions.

- Government regulations may require that you take extra steps to secure the information your business collects. For example, healthcare providers are regulated by the Health Insurance Portability and Accountability Act (HIPAA), which guards against the misuse of personally identifiable health information and limits the sharing of that information. Specifically, you must guard patient information against unauthorized access, alteration, deletion, and transmission. HIPAA compliance is increasingly important as more patient data is transmitted between health care institutions.

- Insurance policies, especially business liability policies, may require specific steps for ensuring the security of data on your computers. Some policies even go so far as to dictate the equipment and procedures that must be in place.

- Special agreements include contracts such as terms of service agreements, which often cover the privacy guarantees you provide to your clients, and non-disclosure agreements, which prevent you from sharing confidential information collected from clients.

When you create a security policy and security plan for your business, make sure you review any regulations, insurance policies, or agreements that may affect you.

For example, a salesperson could use the program to record her sales numbers while a manager creates a customized financial report.

But there are also security risks to such setups. Customer information, sales figures, profit and loss statements, and other vital business data located on a network server are vulnerable to intruders. And you may not want all employees to have access to all kinds of data.

The challenge is to create a security plan that protects LOB program data integrity and privacy, yet also supports efficient data access and collaboration. For more information, see the sidebar "Understand Your Business Requirements."

Basic Steps You Can Take

Protecting your database from unwanted snoopers and other threats starts with establishing basic computer security measures in your workplace. As other security articles point out, you should:

- **Set up firewalls.** Small Business Server 2003, which many small businesses run in combination with their business applications, ships with firewall technology. The premium edition of the server software includes ISA Server—an advanced software firewall solution.
- **Install antivirus software on all computers.** Running antivirus software on your server is as important as running it on desktop computers. Look for antivirus software that detects and disables viruses, and that you can regularly update to screen for new viruses.
- **Use strong passwords.** Passwords should be required to log on to any computer and server in your workplace. Strong passwords have a mix of uppercase and lowercase letters, numbers, and symbols. Require users to change their passwords regularly.

- **Back up files.** Disasters happen, and if you haven't saved your important files and information on a separate storage system, all your critical business application data could be lost. Small Business Server 2003 includes a backup feature that is easy to use.
- **Update your software.** Software updates typically include the latest security features. Updates for Microsoft products are available from Windows Update and from the Microsoft Download Center.

Regulate access to information

Not everyone should have access to everything in your workplace. If your business runs a Windows Server operating system, you can restrict employee access to documents, spreadsheets, or other business files. You can also designate whether a user is permitted just to read a file or to change it. Follow these tips for regulating access:

- Assign permissions and privileges to groups of users rather than to individual users. Doing so saves time administering access rights.
- Create your groups based on roles, such as Sales Representatives. Then, assign a set of permissions that are relevant to performing the tasks defined for that role.
- Set access rights for each group to the minimum levels required for users to do their jobs.

Pay attention to the database

Because business-specific programs typically use a database to store application data, remember to pay special attention to database security. Here are several steps you can take:

- Install the most recent database service packs. The premium edition of the server software ships with the more advanced Microsoft SQL Server™ 2000. When using these database programs in conjunction with your

business programs, make sure to install the latest service packs and updates for improved security. The Microsoft Download Center has the latest server applications updates.

- Assess your server's security with MBSA. MBSA is a free tool you can download and use to scan your standalone or networked computers for security vulnerabilities. With MBSA, you can easily find missing security updates for Windows 2000, Windows XP, and Windows Server 2003 systems. MBSA also works with desktop applications such as Office and server applications such as Microsoft Exchange Server. After scanning your computers, MBSA provides information about locating and installing necessary updates.
- Whenever possible, use existing domain user accounts and passwords for connections to SQL Server databases instead of creating new accounts. Users won't have to remember multiple usernames and passwords, and this technique also helps protect you from most Internet-based attacks against the database.
- Isolate your server and back it up regularly. Physical and logical isolation make up the foundation of SQL Server security. Computers hosting a database should be in a physically protected location. Back up all data regularly, and store copies in a secure offsite location.

Microsoft Business Solutions Customer Relationship Management

Some LOB applications take much of the work out of setting access rights. One example is Microsoft Business Solutions Customer Relationship Management (CRM), a sophisticated program that tracks customer sales and support relationships. Microsoft Business Solutions CRM typically runs in combination with Small Business Server 2003 and comes with eight predefined roles that range from CEO-Business Manager to Customer Service Representative to Marketing Professional.

The program also predefines common business elements to which you can assign rights, such as Leads, Opportunities, Contacts, Accounts, Competitors, Products, Sales Literature, Quotes, Orders, Invoices, and Contracts.

Read More About It

- For articles from Microsoft about securing Line-of Business applications, visit www.microsoft.com/smallbusiness/gtm/securityguidance/hub.mspx
- For downloads available from Microsoft, visit www.microsoft.com/downloads/
- For information about the MBSA, please visit www.microsoft.com/technet/security/tools/mbsahome.mspx

Step 7 Manage Computers from a Server

Without stringent administrative procedures in place, the security measures you take to safeguard your business may be unintentionally jeopardized by users. Just when you think you've followed all the rules to safeguard your business assets against viruses, hackers, and burglars, along comes an employee with an idea that could unravel all the smart security moves you have implemented so far.

As you know, it takes a major commitment to properly safeguard your business from external threats. If you've started that process by updating your software and virus protection and installing a firewall, you've already made a significant investment of time, effort, and money.

Unfortunately, a lack of stringent administrative procedures can unwittingly sabotage that security investment, reversing the changes you've made or inadvertently introducing new risks. Users may not stay current on updates and patches, they may download unauthorized and potentially harmful software, and they may not be vigilant about unauthorized access to data on their computers.

Basic Steps You Can Take

One solution is to manage desktop and laptop computers from your server. Not only will this approach reduce the risk of your security measures being sabotaged, it can also represent a significant savings

in time and money because of the efficiencies you gain, such as:

- **Timely updates.** You can deploy updates and security fixes, along with new versions of software, from the server to users' computers. In this way, you know the updates have been applied properly and in a timely manner, and you don't have to rely on users remembering to do it themselves. You can also test updates before deployment and make sure that computers on the network apply only the proper updates.
- **Special configurations.** If your organization has preferred settings for the operating system or the applications everyone uses, these can be managed, updated, and enforced organization-wide from your server. In addition, you can prevent users from installing unauthorized programs by restricting their ability to run programs from CD-ROMs and other removable drives or to download programs from the Internet.
- **Monitoring.** If unauthorized access or a system failure on a computer occurs, such a situation can be detected immediately through the monitoring capabilities available in a managed environment—a server-based network on which monitoring software is used.

If you're considering a first server or a server upgrade for your business, it's worth noting that improvements in the management capabilities of Windows Server 2003, together with the enhanced security features in Windows XP Professional with SP2, offer a powerful defense against internal and external threats.

Read More About It

- For articles from Microsoft about managing desktop and laptop computers from the server, visit www.microsoft.com/smallbusiness/gtm/securityguidance/checklist/default.mspx
- Find out how Windows Update Services (WUS) can help simplify and automate the deployment of patches and updates at www.microsoft.com/windowsserversystem/sus/

Creating a Security Policy

A security policy sets guidelines that define an organization's approach to security. A policy differs from a plan in that a plan is a call to action, while a policy defines the goals of a plan.

Your security policy will actually be a collection of several different policies, which might include guidelines on employee Web and e-mail use, administrative access, and remote access. A policy is useful only if it's enforced. You should not create policies that are stricter or more complicated than you are willing to enforce. A policy is not set in stone, but is a living document. A good policy must be allowed to grow so that it can accommodate new threats, new technology, and new ways of thinking.

Although each organization's security needs are unique, most security policies address a handful of common elements. (For more information, see the sidebar "Teach Your Employees About Security.") The SANS Institute defines several elements that you should include in a good security policy:

- **Objectives.** This section clearly states the reason the security policy exists.
- **Scope.** This section identifies the people and systems affected by the policy.
- **Protected Assets.** This section identifies the assets that the policy protects. Mail servers, databases, and websites are common business assets that need to be protected. Think of this section as an expanded discussion of the objectives.
- **Responsibilities.** This section of the policy identifies the groups or individuals responsible for implementing the conditions of the policy.
- **Enforcement.** This section of the policy discusses the consequences for violating the policy. Some authorities recommend referring to the appropriate location in the employee handbook as opposed to carrying enforcement directly in the security policy to avoid legal issues.

Teach Your Employees About Security

You can lock down servers and desktop computers, install firewalls, and keep software updated, but one of the toughest parts of securing your business can be getting your employees to follow security guidelines. Fortunately, if you teach your employees why security matters, show them the security policies you have in place and why those policies are there, and encourage them to help enforce those policies, your employees can actually become your first line of defense against intrusion.

- Include your employees when you are creating your security plan. If you make them part of the process, they will be more motivated to help make the plan a reality.
- Hold training sessions for employees in which you teach them important security techniques. In particular, show them how to spot spoofed e-mail messages, make sure that the operating system and antivirus software are kept up-to-date, and use strong passwords.
- You should also teach employees how criminal hackers may try to get information from them. Employees should not leave passwords written down where people can find them. They should also never give out usernames or passwords over the phone—even to someone they think they should trust. Finally, employees should be encouraged not to discuss confidential information or security precautions in public areas. Hackers often try to trick or persuade employees into disclosing confidential information, a technique referred to as social engineering.
- Prepare written policies for employees for using the Internet and e-mail, using company computers for personal projects, and so on. Have your employees sign a copy of the policy so that they understand how serious you are about security. You should also discuss the consequences of not following company policy.
- Continually train new and existing employees on security issues and policies.

Above all, you must communicate with your employees about security. **It should be a topic they hear about frequently so that following good security techniques becomes a habit.**

- **Remote Access Policy.** Outlines acceptable methods for remotely connecting to the internal network, such as whether employees are allowed to connect to the network from their home computers.
- **Information Protection Policy.** Provides guidelines to users on the processing, storage, and transmission of sensitive information.
- **Virus Protection Policy.** Provides baseline requirements for the use of antivirus software as well as guidelines for reporting and containing virus infections.
- **Password Policy.** Provides guidelines for how user-level and system-level passwords are managed and changed.
- **Firewall Security Policy.** Describes, in general, how firewalls are configured and maintained, and by whom.

For more information about security policies, visit www.sans.org

Creating a Security Plan

You need a plan. Security is not a one-off task but an overlapping mesh of technology, people, policies, and processes. A plan coordinates the whole security effort to match your company's security policy and make sure there are no gaps.

There are four steps to creating a good security plan: assess, plan, execute, and monitor. Before you begin these steps, though, your organization needs to develop a simple security policy. First, use the seven-step plan found earlier in this document as a checklist and apply the steps to all the computers in your business. Second, after you have completed the audit, prioritize action items according to the probability and likely impact of a problem. Third, taking each risk in turn according to its priority, decide how to transfer, mitigate, or avoid it (or, on consideration, live with it). Finally, put together a team, allocate resources and responsibilities, and carry out your plan. Monitor your plan to ensure ongoing review and compliance.

A good plan today is better than a perfect plan tomorrow. Planning for security is a cyclical and repetitive process, so it makes sense to execute a quick plan now and refine it later.

Assess

- **Review your own skills and knowledge.** Decide whether outside help or training is required and find a consultant, if necessary.
- **Analyze your current state of security.** Use our questionnaire, seven-step plan, and the MBSA. The MBSA is a free program that scans single systems or multiple systems across a network for common system misconfigurations and missing security updates. View the MBSA at www.microsoft.com/technet/security/tools/

- **Identify assets that need to be protected, such as hardware, software, data, documentation, and people.** Also identify account information, administrative procedures, and legal compliance.
- **Categorize your information according to its sensitivity.** Use the following scale: public (website data), internal (marketing data), confidential (payroll), and secret (patents).
- **Identify required services.** Include services such as remote access and e-mail.
- **Predict threats.** Include threats such as spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege. Consider using trusted third parties to test exposure.
- **Calculate exposure for each asset and service against each threat.** Use the formula ***probability x impact*** = ***exposure*** to generate an ordered list of security priorities.

Plan

- **Remember that the objective is not to eliminate all risk regardless of the cost, but to minimize the risks as much as possible.** There are three main tradeoffs:
  - Functionality versus security required
  - Ease of use versus security
  - Cost of security versus risk of loss
- **For each risk, plan how to transfer, avoid, mitigate, or (worst case) live with it.**
- **Create a plan that:**
  - Includes a policy defining the organization's security requirements and acceptable use
  - Has procedures for preventing, detecting, and responding to security incidents
  - Provides a framework for enforcing compliance
  - Reflects the culture of the organization and the resources available for implementation
- **Create a plan for dealing with a security breach (for example, a virus attack):**

  - What are the goals and objectives in handling an incident?
  - Who should be notified in case of an incident?
  - How will you identify an incident and determine how serious it is?
  - What should happen when an incident occurs?
- **Create a project team. Include management and staff.** Give everyone clearly defined roles and responsibilities.
- **Create a project time line.**
- **Write it all up, and make sure everyone agrees to it.**

Execute

- **Communicate with staff and provide regular training where necessary.**
- **Test measures for technical adequacy and obtain participant feedback.**
- **Modify the plan, if necessary.**
- **Carry out the plan.**

Monitor

- **Research new threats, and include new risks as you become aware of them:**
  - Subscribe to security bulletins.
  - Train users.
- **Modify the plan when changes occur in personnel, the organization, hardware, or software.**
- **Conduct ongoing maintenance, such as virus updates, new user training, and backups.**

For more information about how to assess and manage security risks, see the Microsoft Security Risk Management Guide at www.microsoft.com/technet/security/guidance/secrisk/default.mspx. This guide addresses recommendations for large organizations and for small businesses with stringent security needs. Many of the approaches discussed may be helpful for understanding how to reduce security risks in your small business.

Sample Security Plan: Adventure Works

The following sample security plan was put together by a fictitious company named Adventure Works. Because of the increasing focus on security in the computing world, the company has decided to review security practices and put together a plan to improve those practices. Adventure Works' needs may differ from your company's needs, but reading through its plan should give you a good idea of the steps involved in creating a good security plan.

Adventure Works Security Plan

This plan was developed by Matthew, Managing Director of Adventure Works, in cooperation with other key members of the Adventure Works staff.

Section 1: Introduction

This plan was developed by Matthew, Managing Director of Adventure Works, in cooperation with other key members of the Adventure Works staff.

About Adventure Works

We are a 20-person firm specializing in high-adventure travel packages. Our staff includes designers, travel agents, sales and marketing personnel, and the administrative team that supports them. The staff also includes the senior management of the business: the co-founders, Matthew and Denise, and the financial controller, Steve.

Objectives

This security plan is our first. We will take a broad view of the security risks facing the firm and take prompt action to reduce our exposure. Everyone remembers the virus attack we had earlier this year, and we hope to avoid another disaster like that! However, I hope that by taking a wider view, we may be able to plan for threats we don't know about yet.

I realize that we are limited in time, people, and (of course) cash. Our main priority is to continue to grow a successful business. We cannot hope for Central Intelligence Agency (CIA)-like security, and it wouldn't be good for our culture to turn Adventure Works into Fort Knox. The project team has weighed these constraints carefully in deciding what to do and has tried to strike a balance between practicality, cost, comfort, and security measures. We are all convinced, however, that doing nothing is not an option.

I am taking responsibility for leading this review and ensuring that all the action items are carried out. I am concerned about the risks we face, although having reviewed the plan, I am sure we can address them properly. This project has my full support and is a high priority for the business.

Circulation

Because this document contains important security information, it is confidential. You are requested to keep it under lock and key

when not actually using it, and please don't leave it lying around or make photocopies. We will not be sending this document via e-mail or storing it on the server—paper copies only, please. The following people are authorized to view this document:

- Matthew (Managing Director)
- Denise (Operations Director)
- Steve (Financial Controller)
- Kim (Staff Manager)
- Sutton and Sutton (our lawyers)
- Jeremy (our outside security consultant)

Project Team

The project team includes:

- Denise, project leader
- Steve
- Kim
- Jeremy, advising our staff and carrying out some of the implementation

In addition, we consulted with members of staff from sales, marketing, and design to get their feedback about what they wanted and how the plan might affect them.

Section 2: Assessment Results

Our assessment has produced the following results:

Skills and Knowledge

Our technology consultant, Jeremy, is familiar with the whole situation and will be our expert guide. However, we need to internalize as much of this knowledge as possible by doing as much of the work as we can. Doing so will also help us save money. Luckily, Steve is an amateur computer enthusiast. He has attended a security training course.

Each member of the project team has read the available security planning guides from Microsoft and the Internet Engineering Task Force (IETF) in preparation. The company as a whole is reasonably technically literate, but (with one or two exceptions) they see computers as tools to get the job done and don't know much about how they work.

Our Network and Systems

- **Desktops:** Twenty-two (one per member of staff plus two old machines acting as print servers)
- **Laptop computers:** Six (one each for the directors, one for Steve, and three for the sales team)
- **Printers:** Two (one high-end plotter and one printer-fax combo unit for general use)
- **Servers:** One (running Small Business Server 2003 and looking after files, the Internet connection, e-mail, and our customer database)
- **Internet connection:** 1.5 Mbps cable modem connection

The server and several of the computers are linked by 100 Mbps Cat5 Ethernet cables. The remainder are linked by an 802.11g wireless network with an access port. All computers run Windows XP Professional except for the two print servers and two administrative computers, which run Windows 98.

Security

We compared each computer against the checklist in the Security Guide for Small Business. We also ran the MBSA. These actions produced the following results:

- *Virus protection*: Not present on six computers; not up to date on four computers; generally, most users were aware of viruses but were a bit unsure about what they could do to prevent them.

- *Spam-filtering software*: Many users have begun to complain about spam, but no protection is in place.

- *Firewall*: We thought the ISP's router included a firewall, but it doesn't; so, we don't have one.

- *Updates*: All the Windows XP Professional systems are up to date because they were automatically checking and downloading updates. However, several installations of Microsoft Office need updating, and the Windows 98 computers are not updated at all.

- *Passwords*: A random sampling found that most people aren't using passwords at all or had them written on Post-it notes. In particular, none of the laptop computers are password protected.

- *Physical security*: We had the insurance people in last year, so the window locks, doors, and alarms are pretty good. However, none of the computers have a serial number etched on its case, and we didn't have a log of the serial numbers. We also noticed that everyone, including Tracy and the two directors, are using the same printer, which means that there is a risk of confidential documents being left there by accident.

- *Laptop computers*: All the laptop computers had shiny bags with big manufacturer logos. No security locks.

- *Wireless networking*: We're wide open here. It turns out that we just set the thing up and it worked, so nobody touched any of the settings. The wireless network is open to people who have wireless access capability to snoop on the network or freeload on the Internet connection.

- *Web browsing*: Everyone thinks that having fast Internet access is a great perk, but they are using it all the time and without much thought to the risks. Through a content filtering audit, we found that 20 percent of our Web browsing was unrelated to work. We don't have a policy on acceptable use, and no one is taking any security measures.

- *Backups*: We back up data on the server to a Digital Audio Tape (DAT) drive on a weekly basis, but we haven't tested restoring the data; unless people remember to copy local files to the server, those files aren't backed up, which is unsatisfactory. The server contains our primary customer database, so well-tested backups are essential, as is keeping a copy of backups offsite.

Assets

Besides the physical property, our main assets are:

- Our product designs and marketing collateral
- Records of our contracts with vendors
- Our e-mail database and archive of past e-mail messages
- Sales orders and the customer database
- Financial information
- Line-of-Business (LOB) software for online booking and reservations
- Paper legal records stored in various filing cabinets

All these assets are considered secret and should be accessible only on a need-to-know basis. In addition, they need to be protected and backed up as safely as we can manage.

Risks

We believe the risks break down into four main categories:

- Intruders (viruses, worms, hijacking of our computer resources or Internet connection, and random malicious use). These are the risks that anyone using computers connected to the Internet faces. High risk, high priority.

- External threats (rivals, disgruntled ex-employees, bad guys after money, and thieves). They are likely to use the same tools as hackers, but in deliberately targeting us they may also try to induce members of staff to supply confidential information or even use stolen material to blackmail or damage us. We need to protect our assets with physical and electronic security. High risk, high priority.

- Internal threats. Whether accidental or deliberate, a member of staff may misuse his or her privileges to disclose confidential information. Low risk, low priority.

- Accidents and disasters. Fires, floods, accidental deletions, hardware failures, and computer crashes. Low risk, medium priority.

Priorities

1. Intruder deterrence:
   - Installing firewalls
   - Installing and updating virus protection
   - Strengthening the wireless network
   - Replacing the four computers running Windows 98 with computers running Windows XP Professional with SP2
   - Ensuring that all computers are configured to be updated automatically
   - Educating users and explaining policies
2. Theft prevention:
   - Helping protect laptop computers
   - Inventorying and mark assets
   - Moving the server into a secure, lockable room
   - Physically securing desktop and laptop computers
3. Disaster prevention:
   - Creating better backup plan with offsite storage
   - Ensuring backup of users' local data
   - Storing copies of critical paper documents offsite
   - Regularly testing the backups by performing a restore
4. Internal security and confidentiality:
   - Creating a strong password policy
   - Securing printers for accounts, HR, and directors
   - Reviewing security for filing cabinets and confidential documents

Section 3: Security Plan

After performing our assessment, we have devised the following security plan:

Action Items

1. Select, purchase, and install a hardware firewall (or ask our ISP or technology consultant to provide one).
2. Enable Windows Firewall on the server and on all desktop computers.
3. Make sure that antivirus software is installed on all computers and that it is set to automatically update virus definitions.

4. Configure computers running Office Outlook 2003 to use Junk e-mail filtering. Select, purchase, and install spam-filtering software on the mail server, if necessary.
5. On the wireless network, disable service set identifier (SSID) broadcasting, choose and configure a sensible SSID, enable WPA encryption, enable MAC filtering, and configure the access point to allow traffic only from the desktop and laptop computers in the office.
6. Replace the four computers running Windows 98 with computers running Windows XP Professional with SP2.
7. Review all machines to make sure that they are fully updated, and set them to automatically refresh those updates.
8. Buy new, nondescript laptop computer bags and locks.
9. Security mark all desktop computers, laptop computers, and their components.
10. Log all serial numbers.
11. Buy and install desk security locks for desktop computers.
12. Find a suitable, lockable room for the server and move it there.
13. Review backup and restore procedures. Ensure that user data is either stored on the server or copied across regularly prior to backups. Implement daily backups. Ensure that a full backup goes offsite once a week. Ensure that the backup is password protected and encrypted. Review paper documents and make photocopies for secure offsite storage of critical documents.
14. Configure Small Business Server 2003 and individual machines to enforce reasonably strong passwords. Discuss with users what would be an acceptable balance of convenience and security. (We don't want them writing down their new passwords.)
15. Configure workstations to log users out and require a password to log on again if the workstation is idle for more than five minutes.
16. Buy cheap printers for accounts, HR, and the two directors so that they can have private documents printed securely.

Policy Changes

Kim will update the staff handbook to include new policies on:

- Acceptable use of e-mail and the Internet
- Use of passwords
- Who can take company property away from the office

After she has completed a first draft, it will be reviewed by the directors and the company's attorneys before being rolled out.

User Education

We expect to give up to two hours of user training in small groups as a result of these changes. Training will cover:

- The importance of security
- Passwords
- Laptop computer security
- Virus prevention
- Safe Internet browsing
- Updating software and operating systems from a server
- Introducing the new staff policies
- Making sure employees understand the consequences for not complying with policies
- Assessing employees' understanding of the new policies
- Periodically reviewing the practice of the new policies

Project Time Line and Responsibilities

The top three priorities—firewall, virus protection, and strengthening the wireless network—will receive urgent attention from our security consultant, Jeremy. The remaining tasks will be done by our own staff in order of priority.

We expect the top three priorities to be completed within a week and the remaining tasks within 30 days. Steve will be responsible for purchasing and implementing the technical changes. Kim will be responsible for all the policy and training requirements. Denise will oversee the project and be responsible for any other tasks that arise.

Response Planning

In the event of a security breach, we will contact Jeremy. His company has a one-hour response policy during office hours and a four-hour response policy at all other times to deal with serious incidents, such as virus infections. In addition, Steve will monitor the server and firewall regularly to make sure that no breaches have occurred.

Ongoing Maintenance and Compliance

Steve will be responsible for security on a day-to-day basis, with Denise taking overall responsibility. Steve will continue his own self-education on the topic, subscribe to security bulletins from Microsoft and our antivirus software supplier, and liaise with Jeremy on a regular basis to monitor compliance with the new policies.

On a monthly basis, Steve will make sure that Windows and our antivirus software are updated and that the backup and restore procedures are working properly. He will also be responsible for ensuring that new computer equipment is properly configured and up-to-date.

Kim will be responsible for ensuring that new staff joining the company are fully trained in the company's security policies and procedures.

There will be a full, formal review of this plan in six months.

Section 4: Resources and Budget

The following expenditure has been approved:

Software and Hardware

- Purchase antivirus software.
- Configure Office Outlook 2003 to filter junk e-mail.
- Install a hardware firewall.
- Replace the last four desktop computers running Windows 98 with computers running Windows XP Professional with SP2.
- Purchase security locks and new nondescript laptop computer bags.
- Check into additional backup media.

Professional Advice

- Sutton and Sutton to review our rewritten staff policies
- Jeremy for advice during the creation of this plan
- Jeremy for help with implementation

Internal Resources

- Although we are not paying for our own staff directly, to be clear about the allocation of resources and the time that is available for this work, we have authorized the use of internal staff as detailed above.

Information Online

You should consider this guide a starting point for securing your business. The following sites provide additional technical information and security guidance.

For information about small business technology and security guidance, go to
www.microsoft.com/smallbusiness/
www.microsoft.com/smallbusiness/gtm/securityguidance/

For information about starting and running a small business, go to
www.asbdc-us.org
www.uschamber.com
www.sba.gov
www.entrepreneur.com
http://sbc.nist.gov

For consumer and end-user information, go to
http://safety.msn.com
www.microsoft.com/athome/security/

For business software and productivity solutions, go to
www.microsoft.com/office/
www.microsoft.com/windows/

For server information, go to
www.microsoft.com/smallbusiness/gtm/encomm/freetrial.mspx
www.microsoft.com/smallbusiness/products/server/sbs/detail.mspx

For information about genuine software and the law, go to
www.microsoft.com/genuine/small_business.mspx?displaylang=en
www.bsa.org

For explanations of technical terms, visit
www.howstuffworks.com
www.webopedia.com

For general information about security and safety, visit
www.microsoft.com/protect/
www.microsoft.com/security/
www.microsoft.com/spam/
www.microsoft.com/senderid/
www.microsoft.com/technet/security/topics/hardsys/default.mspx
www.symantec.com
www.isalliance.org

For information about computer crime, visit
www.usdoj.gov/criminal/cybercrime/
www.gocsi.com
www.kensington.com

For mobile networking and VPNs, go to
www.microsoft.com/technet/security/topics/mobile/default.asp
www.microsoft.com/smallbusiness/gtm/mobilize/hub.mspx

For information about backups, go to
www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp

For detailed advice about writing a security plan and for sample policies, go to
www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.mspx
www.sans.org

For information about Internet filtering software, go to
www.websense.com
www.securecomputing.com

For more technical information, go to
www.microsoft.com/security/
www.microsoft.com/technet/security/default.mspx
www.cert.org/tech_tips/home_networks.html
www.ja.net/documents/factsheets.html

For firewalls, go to
www.microsoft.com/technet/security/topics/network/firewall.mspx
www.mcafee.com
www.symantec.com
www.zonelabs.com

For antivirus software and e-mail security, go to
www.grisoft.com
www.symantec.com/smallbiz/nav/
www.mcafee.com
www.pandasoftware.com
www.bitdefender.com

To get software updates for Windows and Microsoft Office, go to
www.windowsupdate.com
www.officeupdate.com

For a complete glossary of security terms, go to
www.microsoft.com/security/glossary.mspx

Microsoft®

Your potential. Our passion.™

www.microsoft.com/smallbusiness

0305 Part No. 099-93165