

Security Strategies for the Midsized Business

Microsoft

Contents

MIDMARKET SECURITY ISSUES	3
The threats.....	3
INTRODUCTION TO MICROSOFT SECURITY SOLUTIONS.....	4
Trustworthy Computing and Infrastructure Optimization.....	4
Risk assessment	4
Conduct a vulnerability assessment.....	5
Prioritize your efforts.....	5
Defense in Depth.....	5
HELP PROTECT YOUR DESKTOPS AND SERVERS.....	6
Step 1—Update operating systems and software	6
Step 2—Use anti-malware software.....	7
Step 3—Implement a host-based firewall	7
HELP PROTECT YOUR DATA	7
Step 1—Take advantage of directory services	8
Step 2—Help protect documents with rights management	8
Step 3—Use encryption for data confidentiality and authentication	8
HELP PROTECT YOUR NETWORK.....	9
Step 1—Install a firewall at the network perimeter	9
Step 2—Implement a public key infrastructure (PKI)	9
Step 3—Implement Internet Protocol Security (IPsec)	9
Step 4—Use virtual private networking (VPNs) for secure remote access	10
Step 5—Secure wireless networks	10
NEXT STEPS FOR SECURITY	11
Educate your users	11
Develop policies	11
Spread the word.....	11
Social engineering.....	11
Contact a Partner.....	12
Conclusion.....	12
ADDITIONAL GUIDANCE.....	12

MIDMARKET SECURITY ISSUES

Midsized businesses face many of the same security threats as their larger counterparts: viruses, worms, malware, unwanted and illegal software, and attacks from both insiders and outsiders. Likewise, they often have to comply with the same regulations that govern vertical industries ranging from health care to financial services.

While they face many of the same issues as larger companies, midsized organizations typically have smaller security budgets, whether for hardware, software and services, or staff. Indeed, in some cases, the IT professional in charge of security in a midsized organization is also responsible for most or all other aspects of the organization's IT infrastructure and networks.

The good news is that security doesn't necessarily have to be expensive. Organizations can maintain a sound security posture by developing—and following—a comprehensive set of security policies and using comprehensive and integrated security solutions when possible. Additionally, a variety of free or low-cost security tools are available to help with everything from risk assessment to routine patching.

The threats

For each of the past 11 years, the Computer Security Institute (CSI) and the FBI have conducted a survey of IT professionals regarding security. The [2007 CSI/FBI Computer Crime and Security Survey](#) is based on responses from 616 computer security professionals in the United States. Nearly half of the respondents work for organizations with fewer than 1,500 employees. According to the survey, the top three security problems are:

- Insider abuse of network resources. This includes problems such as using the Internet for non-work related access or downloading unlicensed software.
- Attacks from viruses, Trojans, or other malware.
- Unauthorized access to computer systems.

These three issues have topped the survey for the past five years—a good indicator that these areas deserve special focus from IT groups.

The survey also finds that the chief sources of financial losses are financial fraud, theft of proprietary information, virus attacks, and theft of laptops and other mobile devices. Theft of proprietary information, which can be any type of intellectual property, is an especially insidious type of attack to defend against. That's because the attack may come not only from an unauthorized intruder, but from a legitimate insider—perhaps an employee who holds a grudge, is looking for illicit profit, or who maybe doesn't realize intellectual property should not be taken to a subsequent job at a competing firm.

INTRODUCTION TO MICROSOFT SECURITY SOLUTIONS

Trustworthy Computing and Infrastructure Optimization

Trustworthy Computing (TwC) is an initiative introduced in 2002, whereby Microsoft pledged to address security issues both in their own software and across the industry. Four pillars—Security, Privacy, Reliability, and Business Integrity—are the basis of TwC.

Microsoft has also developed the Infrastructure Optimization (IO) model to provide customers with a road map to improve their organization’s computing environment through both technology and better management practices. All of these efforts have the shared goal of helping customers bring their infrastructure up to a level where there is resiliency against threats, while also acquiring the agility to move their business goals forward.

The points in the TwC initiative and the IO model should provide organizations with direction for the vision of what they want for their computing environments as they begin to secure them.

Risk assessment

Before you begin trying to secure your IT environment, it is imperative that you know what resources are most important to the organization so you can focus your efforts—and your budget—accordingly. In security terms, this involves conducting a risk assessment.

At the very least, your organization’s president, chief financial officer, and chief information officer should be involved in the assessment. Depending on the size of your company, it may make sense to form a risk assessment committee, with additional members representing different departments and, potentially, the end users who perform everyday functions.

Indeed, the risk assessment must include input from executives representing various organizational business units. They are in the best position to guide you on the data and applications that your organization relies on most.



In [chapter 4 of its Security Risk Management Guide](#), Microsoft provides detailed direction on how to perform risk assessments, breaking the process into three steps:

- **Planning:** Build the foundation for a successful risk assessment by aligning the risk assessment to business processes, accurately scoping the assessment and gaining stakeholder acceptance.
- **Data gathering:** Collect risk information through discussions with stakeholders across the organization. Focus on organizational assets, including a brief description of each and its value to the business, potential security threats, vulnerabilities that may be exploited, and a description of current controls in place and their effectiveness.
- **Risk prioritization:** Rank identified risks in a consistent and repeatable manner.

Ultimately, your risk assessment should answer a few fundamental questions:

- What data and applications are most valuable to your organization?
- Where do your most valuable data and applications reside?
- What will be the impact from a loss of your data or applications, such as downtime caused by a virus attack?
- What is the most cost-effective way to address the risks?

Conduct a vulnerability assessment

Your next step is to conduct a vulnerability assessment by determining where your organization may be susceptible to security breaches. This assessment involves determining which operating systems, services, and other software are running and whether each system has the latest security updates.

Numerous tools are available to conduct vulnerability assessments. These tools automate the process of scanning systems for operating system and security updates and provide reports on their findings.

The [Microsoft Security Assessment Tool](#) (MSAT) is a free tool you can use to help assess weaknesses in your IT security environment. It will also provide recommendations and best practices to help enhance security based on an evaluation of your organization's security practices in such areas as infrastructure, applications, operations, and people. It will help identify processes, resources, and technologies that are designed to promote good security planning and risk mitigation

practices. The tool also compares your organization's risk profile to similar companies, which can help you identify areas where you can better optimize security spending.

While the MSAT tool is free to download, it may be best for midsized businesses to hire an outside consulting organization to help conduct the assessment. This way there will be a certified Microsoft partner on site to answer questions as they arise. Be sure to choose a consultant with specific expertise in the risk assessment area, ideally with companies in your vertical industry.

Another useful tool is the [Microsoft Baseline Security Analyzer \(MBSA\)](#), which scans and assesses your systems directly. This free tool helps small and midsized businesses determine their security status in accordance with Microsoft security recommendations; the tool also offers specific actions you can take to remediate any issues discovered by the MBSA.

Prioritize your efforts

When the vulnerability assessment is complete, the next step is to match the results against your risk assessment. Your goal is to find any systems that house high-value data or applications that are also at high risk of a security breach, as those need to be addressed first. Then you go down the line of securing high-value, medium-risk systems, leaving the low-value, low-risk systems for last. Let your risk assessment guide you in prioritizing which issues to tackle first, always keeping the focus on protecting your highest-value systems. That's where you'll get the most benefit for your efforts.

Defense in Depth

Once you have identified your security vulnerabilities, they can be quickly and cost-effectively addressed by taking a layered approach to security. Enhancing your organization's security with multiple solutions provides redundancy and is referred to in the IT industry as Defense in Depth. Where applicable, this white paper recommends specific Microsoft security solutions that are cost-effective enough to be feasible for midsized businesses, yet robust enough to provide a security-enhanced IT environment. This flexible approach enables midsized organizations to help protect their desktops, their data, and their networks, even with a limited budget.

HELP PROTECT YOUR DESKTOPS AND SERVERS

Protecting desktops, domain controllers, and other servers is typically the primary area of concern for businesses of any size. As the [2007 CSI/FBI Computer Crime and Security Survey](#) and other studies have found, there is a growing prevalence of malicious attacks on systems in the form of malware, viruses, Trojans, maliciously coded Web sites, and phishing.

Another concern is the complexity of centrally managing all aspects of the desktop environment including operating system, software, and update deployment, as well as regulating the adherence to desired configurations.

By taking a few simple steps to help secure your desktops and create an easily managed environment, your company can see immediate benefits such as:

- Reduced time and labor costs for deployment of operating systems, software, and updates.
- Fewer conflicts between applications due to a more uniform environment.
- Increased user productivity due to reduced downtime from malicious attacks or software.
- Simplified management that can give you increased reliability and control over clients and desktop environments, and help you reduce IT overhead.
- Ease of meeting compliance standards.

Step 1—Update operating systems and software

The first step to securing all systems is to install the latest security updates for the operating systems and installed software. These updates fix security issues in the software's code that have been discovered to be exploitable by attackers. As new security issues are discovered, system and software vendors routinely issue software updates to remediate them. Installing updates on a regular schedule is the easiest way to stay ahead of most malware outbreaks.

Regular updating also helps ensure that you are running the latest and most secure versions of applications, such as the Web browser, which is a frequent target. For example, updated versions of Windows® Internet Explorer include an

anti-phishing filter and ActiveX® opt-in, which greatly enhance browser security.

An important preparatory step before installing updates is to test them in a closed environment. By testing the updates before rolling them out to the entire network, administrators can help ensure that the updates don't cause any problems or conflicts with other software, avoiding downtime from unforeseen issues. This test can be done manually by setting aside a small group of machines and checking things by hand, but some tools such as Windows Server® Update Services, mentioned below, can help streamline the process.

The most accessible tool for updating Microsoft® software and operating systems is the Automatic Updates feature included in all recent Windows operating systems. When Automatic Updates is enabled on client machines, high-priority updates for supported Microsoft products are automatically installed, free of charge. Updating tools enable you to schedule updates and enable required restarts in order to make the process all but transparent to end users. For larger organizations, it will quickly become useful to be able to distribute updates from a central location across your entire organization, rather than just relying on Automatic Updates. Numerous tools are available to help you do this. They include [Windows Server Update Services \(WSUS\)](#), which is available at no cost, as well as various third-party security update tools. If a tool such as WSUS is used, then Automatic Updates will serve no additional purpose, and should be disabled.

The most robust tool for midsized businesses is [Microsoft System Center Essentials \(SCE\) 2007](#). SCE consolidates not just updating services, but a wide range of system management tasks into a single console including:

- Software deployment
- System monitoring and reporting
- Troubleshooting
- Hardware and software inventory

Regardless of what tool you choose to do it, regular updating is crucial. It cannot be overemphasized how important it is to keep all software and operating systems on all desktops and

servers updated as often as possible, as this is the only way to keep up with new threats, which arise continually. A good way to stay abreast of all these threats is to subscribe to the bulletins in [Microsoft Security Notification Service](#), and sign up for the monthly security newsletter.

In addition to applying regular updates to existing operating systems and applications, midsized businesses should consider upgrading to the latest versions of desktop operating system and productivity software that include added security features. For example, Windows Vista® includes User Account Control (UAC) to address the risk of logging on with administrative privileges, and the 2007 Microsoft Office system uses a new, more secure XML-based default file format. Visit the links at the end of this white paper for more information about the new security features in Windows Vista and the 2007 Office system.

Step 2—Use anti-malware software

Malicious software continues to be a growing security concern. According to the 2007 Malware Report from Computer Economics, lost user hours, system downtime, and remediation proved costly. Anti-malware and malware removal software is the most direct approach to dealing with malware. When systems have the proper updates installed, your next step is to help ensure they stay protected by installing software that can help protect against various forms of malware, notably viruses and spyware. An effective anti-malware program will help protect your systems against most viruses, spyware, worms, Trojans, and other malware.

Anti-virus and anti-spyware programs are available from numerous vendors, including Microsoft. Most leading anti-malware applications can be configured to automatically download updated signatures, enabling them to thwart the latest attacks. Windows Vista comes with Windows Defender, an anti-malware tool that offers a Real-Time Protection monitoring system that recommends actions against detected malware. If your organization is looking for a more robust solution that includes both anti-spyware and anti-virus technology, Microsoft Forefront Client Security can help protect both desktops and servers. Some smaller organizations might find [Windows Live™ OneCare™](#) to be a good solution because it combines virus

scanning, file backups, firewall, print sharing, and management of multiple systems all in one package.

Step 3—Implement a host-based firewall

A system's first line of defense against network worms and other network-based attacks is the host-based or personal firewall. This software, which runs on each computer, controls network traffic to and from the computer. This differs from a perimeter firewall (discussed later) as a host-based firewall helps protect the individual system on which it is installed. Even if a perimeter firewall is already in place, you can improve your security posture by installing personal firewall software on every system in the organization.

The simplest and most cost-effective solution for most organizations is Windows Firewall, a feature of both Windows XP and Windows Vista. Windows Firewall also includes advanced configuration options and the ability to filter outbound traffic. Another advantage is that it can be managed via Active Directory Group Policy, reducing the administrative overhead of managing the personal firewall configuration throughout your company. The [Microsoft Firewall Services Implementation Guides](#) on TechNet provide additional guidance on firewall selection and implementation.

HELP PROTECT YOUR DATA

The essence of data security is in the three major components of the CIA Model: Confidentiality, Integrity, and Accessibility. Unauthorized data access from employees and network security breaches continue to be a large security concern, and organizations must protect themselves from data loss due to physical theft and hardware, software, or user error. The CIA model helps organizations protect their data by helping them ensure that data only reaches intended users, can be verified to be unaltered, and is available on-demand to authorized users. Implementing a more comprehensive and integrated solution to data protection can provide:

- Increased user productivity by eliminating the downtime caused by loss of data.
- Increased IT productivity by reducing the time spent involved in servicing user data restoration requests.
- Decreased financial losses due to stolen or misused data.

Step 1—Take advantage of directory services

Directory services play a crucial role in ensuring that only authenticated and authorized users are able to access your computer systems. As your business grows, keeping track of users and the systems they are allowed to access can become increasingly complex.

A directory helps streamline identity management tasks by giving you one place in which to store all group and individual access rights. A single directory is generally considered to provide better security than defining access rights in various access control lists or on an application-by-application basis. Without a directory, access rights information can quickly get out of sync. A major risk of out-of-sync databases is that an employee who has been fired may not have his or her accounts removed from all databases, making it possible for him to leverage that account in an attack against the company.

Using Active Directory and Group Policy

Organizations with network infrastructures built on Windows domains should use Microsoft Active Directory® for directory services. Active Directory was introduced in Windows Server 2000 and is included in Windows Server 2003 and Windows Server 2008. Active Directory enables centralized, security-enhanced management of an entire network, even one that spans multiple physical locations. Organizations can use Active Directory to define specific user groups and the resources that each group is allowed to access. When you assign an individual user to a group, the user automatically gets access to all the resources defined for that group.

In Active Directory, Group Policy drives configuration options, enabling you to more easily deal with groups of users and their specific requirements. Group Policy can also be used to define specific security settings and help ensure that users adhere to them. For example, you can set a Group Policy so users adhere to a password policy dictating that they must change their login password every 90 days. Similarly, you can use Group Policy to enforce restrictions that prevent users from loading unauthorized applications, among many other security-related features.

Microsoft offers extensive, free guidance for how to effectively implement Active Directory and Group Policy. The [Medium Business Solution for Management and Security Using Active Directory Group Policy](#) guides explain how to plan, build, deploy, and operate advanced Active Directory features in a midsized IT environment.

Step 2—Help protect documents with rights management

While there are many networking technologies and policies designed to prevent unauthorized users from gaining access to sensitive data, none of them will help in the all-too-common scenario of a legitimate and authorized user accessing a sensitive document and then sharing it, maliciously or not, with unauthorized users.

Rights management controls address this issue by granting permissions to individuals, groups, computers, or trusted applications for common actions, such as reading, copying, or printing.

The Microsoft implementation of rights management is Information Rights Management (IRM) in the 2007 Microsoft Office system. To use IRM, Windows Rights Management Services (RMS) must be installed both on the client and server sides. Consult TechNet for extensive [guides](#) on implementing and using IRM and RMS.

Step 3—Use encryption for data confidentiality and authentication

As numerous public cases have recently exposed, if a laptop containing sensitive data is lost, it can leave an organization at significant civil and potentially criminal risk. The most common way to protect valuable data is encryption. While encryption was once considered an intrusive, computing-intensive chore, it can now be performed in the background, with little to no noticeable effect on performance. This makes encryption a viable option for helping to protect your most sensitive data, whether it's at rest or in transit across your network. Encryption technology can also be used to provide authentication by validating the identity of the content creator or sender. Encryption can also play a key role in helping protect data stored on laptops.

Microsoft Encrypting File System (EFS) technology, a component included in Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008, makes it easy for users to individually encrypt and decrypt files. The 2007 Office system also includes encryption technologies that enable users to digitally sign documents for authentication, password protect documents for confidentiality of content, and sign and encrypt e-mail messages sent via Microsoft Office Outlook® 2007.

Windows BitLocker™ is a feature new to Windows operating systems, introduced with Windows Vista and Windows Server 2008. BitLocker helps protect the data on systems that may have been lost or stolen by encrypting the entire Windows system volume, and by verifying the integrity of the boot sequence. Encryption must be well understood and managed to avoid the potential loss of important files. For example, you should implement a key archival system to protect keys—and the files they are associated with—from being lost. This can involve simply storing the keys on a CD-ROM and storing it in a safe place.

HELP PROTECT YOUR NETWORK

Viruses, malware, spam, and Denial of Service (DoS) attacks affect more than just one facet of a company's assets. Therefore, a good network security plan will include multiple layers of security, covering client computers, server infrastructure, and the perimeter. This Defense in Depth (DiD) strategy will establish a more secure network, providing numerous benefits:

- A more stable, secure, and reliable infrastructure.
- Quick and reliable delivery of security updates, creating a faster response time to emergent security threats.
- A more controlled and secure environment better able to withstand attacks.
- Reduction in hardware and software operational complexity, creating an easier administrative environment.
- Fewer requests for assistance from users due to security exploits, such as unwanted software or Trojans.

Step 1—Install a firewall at the network perimeter

The first line of defense for an organization's network is the perimeter firewall. Unlike the personal firewalls mentioned earlier

that help protect clients, perimeter firewalls inspect and control inbound and outbound network traffic in the zone that links an organization's private internal network with the public Internet.

Types of perimeter firewalls are extremely varied. They can range from a simple combination firewall/router device to a full-fledged dedicated firewall appliance or server. The Microsoft edge firewall solution is Microsoft Internet and Acceleration Server (ISA), which can be purchased as an appliance or installed on a standard Windows Server computer. Microsoft offers extensive information about choosing and implementing a perimeter firewall in the [Perimeter Firewall Design Guide](#).

Step 2—Implement a public key infrastructure (PKI)

Many of the network security technologies that make up the layers of a DiD strategy depend on digital certificates and public/private key pairs. A PKI consists of one or more Certification Authorities that issue certificates binding keys to users or machines.

A private PKI will enable you to avoid the costs associated with obtaining certificates from a public CA, and give you greater control over key storage, revocation, and other aspects of administering the PKI. Windows Server operating systems include Microsoft Certificate Services, which enable midsized organizations to easily and cost-effectively take on the role of CA.

A comprehensive guide for implementing a PKI can be found [here](#).

Step 3—Implement Internet Protocol Security (IPsec)

IPsec is an open framework of security standards for encrypting transmissions across the network. IPsec allows two network peers to authenticate to each other using pre-shared keys, digital certificates, or Kerberos protocols within an Active Directory forest. After the computers authenticate each other and establish traffic signing parameters, IPsec helps ensure communications are tamper free and private.

IPsec support is built into Microsoft server and client operating systems and is automatically implemented in IPv6. Midsized businesses will benefit from reduced administrative overhead by centrally managing IPsec policies using Active Directory Group Policy.

IPsec is a mature technology and there are many resources available to guide implementation, including the Microsoft [Overview of IPsec](#).

Step 4—Use virtual private networking (VPNs) for secure remote access

Most organizations need to provide secure access to their computing resources to users who are outside the walls of headquarters. Whether that entails providing connectivity to branch locations, traveling users, or business partners, there are security considerations when enabling your employees and partners to work remotely or in branch offices.

Often the simplest, least expensive way to provide secure connectivity is to establish virtual private network (VPN) connections. VPNs enable you to employ relatively inexpensive Internet connections that link remote locations with your headquarters; in essence, a security-enhanced, encrypted tunnel across the Internet through which your corporate data travels.

Numerous types of VPNs are available, most notably those based on the IPsec and SSL protocols. Windows Server 2008 includes a built-in VPN server so you can easily implement an IPsec or SSL-based VPN server at no additional cost. For more sophisticated VPN deployments that require enhanced access control and application security, Microsoft ISA Server 2006 provides a cost-effective unified firewall and VPN solution with fundamental support for branch offices. Larger organizations that have branch offices will also find Microsoft Intelligent Application Gateway (IAG) 2007 to be a useful solution. IAG 2007 provides integrated support for SSL-based VPN access, a Web application firewall, and a management system to provide remote access control, authorization, and content inspection for a large number of business applications. IAG 2007 and ISA Server can also be consolidated into a single appliance that provides comprehensive perimeter security and remote access.

Step 5—Secure wireless networks

If your organization employs wireless LANs (WLANs), there may be an additional layer of vulnerability to your perimeter security concerns. WLANs can, in effect, extend your network perimeter far beyond the walls of your building. Intruders equipped with packet-sniffing tools can search for WLAN signals from the parking lot outside your building and, if your network is not properly secured, they can have easy entry to your corporate resources.

Traditionally, WLANs used the Wired Equivalent Privacy (WEP) protocol to encrypt transmissions. However, the best security practice is to use a stronger protocol such as Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access Version 2 (WPA2). Windows XP SP2 and Windows Vista clients include built-in support for WPA and WPA2 along with WEP. For additional security, Microsoft offers a [guide](#) that can help medium-size companies implement relatively simple yet effective wireless security using passwords and the Protected Extensible Authentication Protocol (PEAP). Windows Server 2008 includes the Network Policy and Access Server (NPAS), a RADIUS server you can use to deploy PEAP secured Wi-Fi access at no additional cost.

With this solution in place, a wireless client device seeking WLAN access would first authenticate over a secure channel to a RADIUS server. If the client successfully authenticates, the RADIUS server delivers the keys required to establish a secure, encrypted wireless connection. With such a system in place, intruders will be unable to authenticate to the network and packet sniffers will be unable to pick out your data.

Additional step: network access protection

A major threat to networks comes from remote, non-company owned clients that connect to the internal network via VPN, such as an employee's home computer. Many home computers do not have the latest security updates applied and may not be running anti-virus software and firewalls, enabling malware and attacks to enter your company network through them. Therefore, it is important to screen all computers that connect to your company's network and block those that may pose a threat.

Network Access Protection (NAP), built in to Windows Vista and Windows Server 2008, is the Microsoft solution for enforcing compliance with network security policies. NAP is a powerful system that inspects a client computer's health status, including software updates and anti-virus signatures, and grants or denies access to the network. Organizations can also set up a quarantined area for non-compliant computers to install or update the software needed to gain compliance.

NEXT STEPS FOR SECURITY

Educate your users

As noted earlier, maintaining tight security depends as much on policies and procedures as it does on deploying technology. With that in mind, establishing security policies and educating end users needs to be a primary—and ongoing—concern. Microsoft provides a tremendous amount of free information about security education at www.microsoft.com/security.

Develop policies

- **Internet use:** Educate your users on what is considered inappropriate Internet use and remind them that the Internet is to be used primarily for business purposes.
- **E-mail:** In addition to reminding users that e-mail is to be used for company business, you should also advise users not to click attachments if they are unsure of the sender or content.
- **Passwords:** Establish policies around password strength and the frequency with which passwords must be changed.
- **Sensitive documents:** Employees must be aware of what kinds of documents are considered sensitive and how to treat them.
- **Anti-virus and firewall use:** Sophisticated users may be tempted to change anti-virus and firewall settings, or to disable them entirely at times. Your policy should be clear that such activities are not allowed.
- **Remote access:** Many users need access to corporate systems when they are traveling or working from home. Your policy needs to acknowledge this requirement, while also establishing safeguards, such as dictating a minimum level of security for any machine used to access corporate resources.

Spread the word

Written policies won't do any good if users don't know about them or don't follow them. So once you've set your company

policies, the next step is to educate your users. The best course of action is to instill in users a sense of responsibility for doing their part to keep the company secure. This will be an ongoing exercise, as no single company memo or training session will likely be sufficient. Rather, security is a message that bears repeating time and again.

Security training doesn't have to be onerous or ominous. An effective way to drive the point home is to hold informal, lunch-time training sessions in which IT executives or a third-party training company educates users about what can happen if security breaks down.

It should also be clear to employees that your security policies have the backing of upper management. That can be accomplished by having the CEO distribute the policy, and by requiring employees to sign off that they have read and understood the policies. It's also effective to have management representation at training sessions to explain the importance of security to the organization.

Social engineering

Social engineering attacks deserve special consideration in your security training. Even the most stringent security often cannot withstand an effective social engineering attack, such as when an attacker dupes an authorized company insider into divulging sensitive information like passwords. Often these attackers pose as IT personnel performing "upgrades" or troubleshooting a problem.

Security training should include examples of common social engineering attacks so that users can recognize them. Encourage users to be wary of anyone asking for sensitive information such as passwords. Let them know under what circumstances, if any, IT would ever legitimately ask for such information.

Microsoft offers a free [security awareness toolkit and guide](#) package that can help you design a training program that works for your organization. The package includes presentations with content you can leverage to create security awareness training

programs for your organization. It also includes numerous templates for creating presentations, brochures, and posters to help with your security awareness efforts.

Contact a Partner

It is highly recommended that midsized businesses contact a qualified Microsoft Partner for consultation before implementing a specific security plan. These experts will be extremely useful for the risk and vulnerabilities assessments, as well as for recommending the best security strategy tailored to your company's specific needs. The [Microsoft Resource Directory](#) can help you find a Security Solutions–certified partner in your area.

Conclusion

Following the layered approach to desktop, data and network security should help establish a sound, cost-effective foundation for your organization. But maintaining proper security requires consistent attention to issues including:

- **Systems management:** Timely installation of patches to all systems is crucial to proper security; an automated patch management system is a great help in this regard.
- **Vulnerability assessments:** As your network changes, so does your security posture. Running a tool such as MBSA once per month will help you identify any systems that may have fallen out of compliance. Similarly, conduct a vulnerability assessment at least once each year to find any holes. Consider hiring an outside consultant for the task, as such a consultant is likely to find more holes than you will on your own. The results of an objective, third-party test can also help you lobby executives for additional security funding.
- **User training:** New employees should receive security training as part of their orientation, and existing users should receive repeated reminders about security best practices. Establish a security training schedule for your employees and stick to it. Take advantage of the various resources available from organizations such as Microsoft and the [SANS Institute](#).
- **IT training:** IT personnel, too, need to be updated on the latest security threats and best practices. Don't leave yourself out of the training regimen.

Implementing proper security is a process and, as such, the job is never really complete. Intruders are constantly searching for new ways to break into corporate networks. Vigilance in adhering to security best practices is your best defense.

ADDITIONAL GUIDANCE

For further education on the security issues confronting businesses today, administrators and IT professionals can browse the [Security Events and Webcasts](#) home page to find upcoming webcasts or events in their area.

This section provides links for solutions mentioned in the document, and more prescriptive guidance for implementation:

The Microsoft Midsized Business Security Center has resources to help protect your company from viruses, hackers, and other threats, all tailored specifically for midsized businesses.

<http://www.microsoft.com/midsizebusiness/security>

Additional resources for midsize business security:

<http://www.microsoft.com/technet/security/midsizebusiness/default.aspx>

The Microsoft Software Asset Management page offers information about conducting a software inventory, including a list of automated inventory tools.

http://www.microsoft.com/resources/sam/sbs_1.aspx

The Microsoft Education piece, "Understanding patch management options for student computers," also applies to midsized businesses with remote sites.

http://www.microsoft.com/education/student_patch_management.aspx

Resources and documentation on Microsoft Windows Server 2003 Active Directory.

<http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.aspx>

A primer on firewalls, including the different types and how to configure them.

<http://www.microsoft.com/technet/security/guidance/networksecurity/firewall.aspx>

Conducting a risk assessment: Chapter 4 of the Microsoft Security Risk Management Guide:

<http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/srsgch04.aspx>

Securing Wireless LANs with PEAP and Passwords:

http://www.microsoft.com/technet/security/guidance/cryptographyetc/peap_0.msp

[The Medium Business Solution for Management and Security using Active Directory Group Policy](#) includes guidance that can be used to plan, build, deploy, and operate advanced Active Directory features like organizational units (OUs) and Group Policy objects (GPOs) in the medium IT environment.

The guidance includes a wide variety of scenario-based configuration schemes, as well as guidance on secure passwords.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=bb534b41-b413-4483-9097-879f5cafe2dc&DisplayLang=en>

[Medium Business Solution for Core Infrastructure v 1.0](#)

This installment of the Medium IT Solution Series, which is targeted at growing businesses with 50 to 250 users, includes the main office and the branch office LANs, the network and directory services, secure Internet connectivity, and file services.

<http://www.microsoft.com/downloads/details.aspx?FamilyId=A3E1B8FC-D67B-4F1C-B969-482D163C1A37&displaylang=en>

Microsoft offers a free [security awareness toolkit and guide](#) package that can help you design a training program that works for your organization.

<http://www.microsoft.com/technet/security/understanding/awareness.msp>

Windows Server Update Services, a free automatic updating system for Windows Servers and Clients can be downloaded at:

<http://technet.microsoft.com/en-gb/wsus/default.aspx>

Security in Windows Vista homepage:

<http://www.microsoft.com/security/windowsvista/default.msp>

Security Guide for the 2007 Microsoft Office system:

<http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/securityguide/default.msp>