GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Small Business Guide to Network Security

Bob Clark
June 11, 2002
GSEC Practical v1.3

ABSTRACT

Small businesses represent more than 99% of all employers, employ 51% of private-sector workers, and provide 51% of private-sector output. These small businesses utilize technology in their daily existence but do so with limited IT resources in both dollars and technical staff. The advent of broadband Internet, off-the-shelf software packages, and low-cost technology has given many of these companies the ability to access information, resources, and clients in a method similar to large enterprise companies. This use of technology has made small businesses susceptible to the same computer and network security threats once considered issues of large corporations.

With a lack of IT resources, especially security, these small businesses often fail to provide a cohesive process by which network security is analyzed, implemented, and managed. This leads to products and applications being installed with default settings and without consideration given to security. Sometimes businesses notice security breaches when their Web sites are defaced or a virus causes damage, but more often the unprotected systems are unknowingly compromised and teamed together to provide a distributed attack against larger targets.

Many of the issues facing small business arise because small business owners and IT staff have not been introduced to the key security concepts and terminology. Security papers are written for IT specialists in large enterprises; they are not written for the average small business technician or owner. Also, security checklists often cover only one layer or area of security.

By compiling information from many resources and customizing it for the small business environment, you find that all small businesses face common vulnerabilities that, when mitigated, will protect small businesses from the majority of threats they face. Twenty-four practical defenses covering the security spectrum—from physical security to data security—are needed for all small businesses. Education of the key concepts and terms of security along with practical security defenses allows a small business to provide a successful, secure computing environment with limited time and resources.

INTRODUCTION

Small business security is often implemented by following any number of currently published security checklists. These often only pertain to a narrow component of network security and are offered as the end-all be-all solution. Small businesses with the lack of resources and time find these checklists helpful and believe that by following them they are protected. This provides a false sense of security, which can be more costly then no security at all.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There is nothing wrong with these checklists. They can be very useful when a person has a clear understanding of what they are trying to accomplish. If I wanted to focus on security from the latest virus threats, a checklist for protection from viruses would be useful. Education and understanding are key. When a small business understands the components of security and how they are applied they can utilize these checklists in a beneficial manner.

I have compiled in this paper a general overview of security terms and practices along with 24 practical defenses that all small businesses should implement. This culmination of information has been compiled from many resources, customized for small business, and is flavored with my experience in consulting small businesses for the last 5 years. This is not the silver bullet for small business security, but it does provide a holistic security framework to protect from the greatest number of threats and provides education on security so that these items can be implemented not haphazardly, but with thought and understanding.

UNDERSTANDING SECURITY

Small businesses need to begin by educating themselves on the general components of security and how they relate. My goal is to provide a basic overview of security that can be used with the security defenses contained in this document to provide small business with not only a holistic checklist but also the education to understand the importance of the security and the practices to mitigate specific risks their business faces.

The term security itself is commonly defined as management of the risks your business faces. All business faces risk in one form or another, and it is not practical to completely eliminated risks. Higher levels of security often impede upon on functionality and have a high cost to implement and maintain.

For example: If you had a single computer and wanted to increase security from e-mail viruses you could choose to never have that computer connect to any other computer or to the Internet. That would make it secure from e-mail viruses but at the same time it has now lost the functionality of communicating via e-mail.

This is where risk management plays a role to determine what is at risk, what level of risk is acceptable, and what is the value of the resource you are trying to protect. "You would not use standard door locks and a home alarm system to guard the Crown Jewels."[1]

To better understand security you must familiarize yourself with the following terms: Resources, threats, vulnerabilities, exploits, and defenses, and how they fit in the risk management and assessment process.

Resources

A resource is anything you are trying to protect. Resources typically include systems, applications, data, and people. Security is the protection of these resources. An important consideration when managing the risk to a resource is to consider its value. This will

[1] *Microsoft Security Operations Guide for Windows 2000 Server*, p.10.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

often be used to determine the level of security to implement; e.g., an online e-commerce Web site that produces five thousand dollars of revenue per day would require greater security than a standard brochure-type Web site providing only basic company information.

Threats

A threat is anything that can inflict harm to a resource. Threats come in various forms and can be categorized as follows:

Table 1 Threats to Small Businesses[2]

Threats	**Examples**
Natural Disasters	Floods, Fires, and Earthquakes
Non-human	Product failure Power failure
Human	*Non-Malicious:* Human Error (Deleting files), Accident *Malicious:* Viruses, Hackers, Thieves, Disgruntled employees

Every business has different threats and part of a risk assessment is to identify these threats. For example, a small business that operates in a highly specialized field may have a malicious human threat from industrial spies, whereas most other small businesses would not.

Vulnerabilities

Vulnerability is a weakness that makes a resource susceptible to loss. These weaknesses must be mitigated to provide security. It is not always practical to remove or reduce the threats but to focus on eliminating vulnerabilities.

Typical small business vulnerabilities can be categorized as follows:

Table 2 Vulnerabilities to Small Businesses[3]

Vulnerability Categories	**Examples**
Physical / Environmental	Unlocked server room Broken alarm system or airconditioner
Software	Un-patched software or Out-of-date virus definitions
Hardware	Clone equipment Lack of redundant hardware
Human	Lack of training and misadministration Unauthorized disclosure

[2] *Microsoft Security Operations Guide for Windows 2000 Server,* p.10.
[3] *Microsoft Security Operations Guide for Windows 2000 Server,* p.11.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Communication	Wireless networking Undocumented cabling or devices Unencrypted communication over public networks
Media	Removable storage such as backup tapes, zip disks, or even paper documents

It is important to keep in mind that resources have weaknesses in many categories. For example, a basic network server may have the following vulnerabilities:

- Be in an unlocked server room—vulnerable to theft or access by unauthorized personnel.
- Have un-patched software—vulnerable to hackers and worms
- Not have redundant hardware—vulnerable to equipment failure

Exploits

Exploits are the actual attack against a weakness in a resource. A hybrid attack is one that uses multiple exploits to gain access to data or equipment. These hybrid attacks begin with information gathering and social engineering proves to be a very reliable method. It is amazing what a person will tell a complete stranger about their network.

Table 3 Exploit Examples[4]

Exploit	**Examples**
Technical Vulnerability Attacks	Buffer overflows Brute force attacks Use of default settings / Misconfiguration
Information Gathering	Network sniffing / Port scanning Social engineering Document grinding / Dumpster diving
Denial of Service	Resource exhaustion Configuration modification Physical damage or theft

Loss is what occurs from an exploit. Loss is represented in the terms of confidentiality, integrity, or availability.

Table 4 Loss Examples[5]

Loss from Exploit	**Example**
Confidentiality	Unauthorized access Impersonation Elevated privileges Public disclosure
Integrity	Data corruption Misinformation or inaccuracy

[4] *Microsoft Security Operations Guide for Windows 2000 Server,* p.11
[5] *Microsoft Security Operations Guide for Windows 2000 Server,* p.12

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Availability	Denial of service Theft or destruction

A simple example would be that an internal user with improper security rights accidentally deletes critical data resulting in either an availability or integrity loss. Availability loss occurs due to denial of service because the data is lost, or integrity can be compromised if partially deleted data causes misinformation or data corruption.

Risk Assessment

Risk management requires the assessment of risk. This is accomplished in the relationship between threat and vulnerability. Threats and vulnerabilities can be assessed in either a quantitative or qualitative fashion.

A quantitative assessment example: Your retail store accepts personal checks for payment on purchases. You sell $100,000 a month of which 40% is tendered by check. You have a 1% bad check rate. This means that accepting checks for payment results in a direct loss of $400 per month. You can then evaluate that against the cost to reduce the vulnerability. You could subscribe to a check verification service that charges 1.25% on each check, which comes to $500 per month. This results in costing you $100 more then having the higher vulnerability. It is clear that for right now, accepting the risk of not having a check verification service makes sense.

Not everything can be put in a quantitative formula, nor should it be. Most network threats and vulnerabilities have to be approached in a qualitative fashion.

The qualitative assessment can be easier to evaluate. It is done by assigning a level to both the threat and vulnerability, such as low, medium, or high. Then, by using the matrix below, you can determine the level of risk that is posed.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

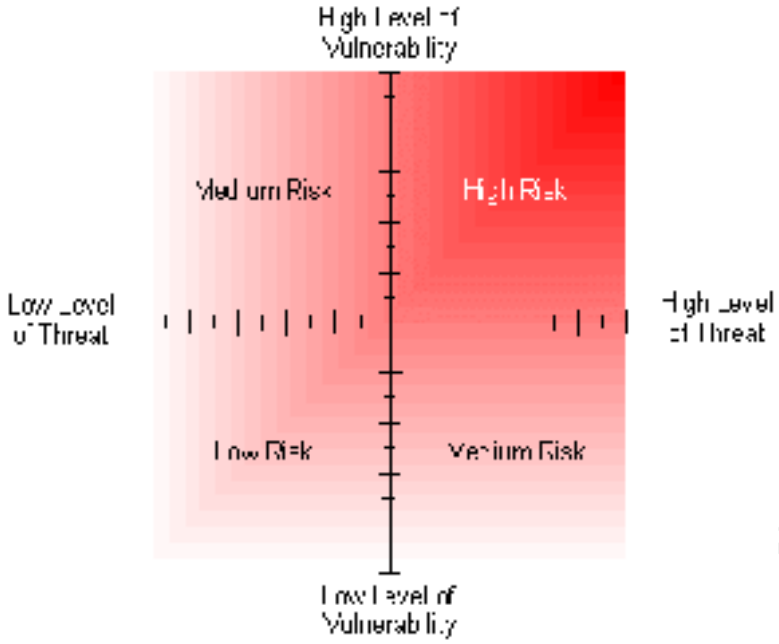


Figure 1 Risk Matrix[6]

Defenses

Defenses are deployed to defend your resources from attack. They are used to lower your risk by reducing threats or vulnerabilities. The approach to deploying defenses is to layer them, creating a multi-layered security fabric that is invulnerable to a single point of failure. This is commonly referred to as a defense-in-depth strategy.

DEFENSE-IN-DEPTH

By layering security measures, failure or compromise of a single defense does not allow direct access to the protected resource. For example, if an attacker were able to compromise a firewall there would be additional layers of security to prevent access to sensitive data resources.

[6] *Microsoft Security Operations Guide for Windows 2000 Server*, p.13.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

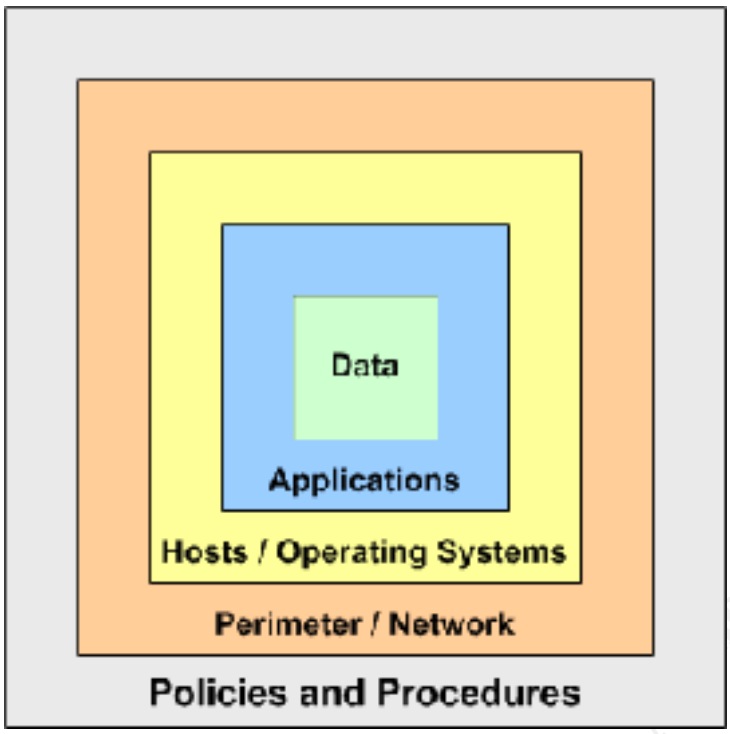


Figure 2 Defense-in-Depth Security Layers for Small Business

A small-business network has many layers in which security can be applied. As we see in Figure 2, the network is comprised of identifiable partitions. It is important to recognize at which layers defenses can be implemented to protect from specific threats and vulnerabilities.

Viruses are very destructive because they can attack a network at many layers. The Nimda virus, for example, exploits vulnerabilities at the perimeter, operating systems, and applications layers. This results in the need to have layers of defense to protect from just this single threat.

Small Business Security in Action

There is an important rule regarding information security called the 80-20 rule. "This rule states that 80% of security risk is effectively managed by implementing the most important 20% of available technical security controls. Small businesses benefit greatly from this rule in that effective security can be implemented to protect from 80% of the threats by deploying defenses to 20% of the vulnerabilities. I will identify the 20% of vulnerabilities that affect small businesses and offer defenses to provide a defense-in-depth strategy.

Before we look at the specific layers of security and appropriate defenses, we need to define the approach to security. The approach and guidelines are contained in a document called the Security Policy. Many small businesses fail with security due to a lack of a security policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Policy creation is not the focus of this paper, but it is an important part of an effective security strategy. You need to review this security policy information and use the links provided to create the policies for your company.

SECURITY POLICY

As shown in Figure 2, the security policy and procedures provide the written guidelines to the application of security and its application to the layers of security. A security policy is made up of a general policy and many issue- or system-specific policies. There are many great resources to help you create policies for your company. I will present some ideas in regard to the policies, but there are many other aspects of a policy that need to be included, such as purpose, background, scope, and responsibility.

General Policy

The general policy is a high-level policy that states the tone and approach to security. It can be as simple as XYZ Company will provide a satisfactory level of security to protect the integrity, availability, and confidentiality of the data and systems that comprise the IT infrastructure.

Without a policy and a statement such as this, would any of your staff understand the level of importance security plays at your company?

Specific Policies

Now, based on your risk assessments, you should create issue- and system-specific policies to address your items of particular interest.

The specific policies that all businesses should have are:

Table 5 Policy Guidelines

Policy	Guidelines
Anti-Virus	• Use the company standard anti-virus software • Maintain current anti-virus definitions • Never open macros or attachments from unknown or untrusted sources • Never download files from untrusted sources • Report virus detection immediately
Passwords / Accounts	• Enforce strong passwords • Require password changes at regular intervals and do not allow reuse • Rename well-known accounts, such as Administrator and Guest • Remove inactive accounts • Do not reveal passwords to anyone

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Data Backup	• Frequency, method, and data sets • Storage of media (offsite) • Rotation and retention • Documentation • Recovery testing
Proprietary Information	• Access to information is on a need-to-know basis • No distribution outside of company without consent • Guidelines for proper disposal • Penalty for deliberate or inadvertent disclosure
Internet / E-mail / System Usage	• Use only licensed software • Use of Internet or e-mail for illicit or illegal activities is not allowed • Electronic communication is not considered private

The SANS Institute has an exceptional resource of guidelines and templates for use in creating policies (www.sans.org/newlook/resources/policies/policies.htm.)

SMALL BUSINESS NETWORK SECURITY

We will begin on the outside of our network or physical environment and work our way down to the data. This approach allows the first layers of defense to protect from the greatest amount of threats. We can compare this to securing a house where we install a fence around the house and limit access through a gate. We then can add locks on the gate, door and locks on the house, alarm system on the doors and windows, a safe in the house, etc. I think you get the picture.

I'll show the defenses that most any small business should employ. Every business is different, and based upon your own risk assessment, you should customize any additional defenses to effectively manage your risk. This is a broad-brush approach to security and is by no means a comprehensive program for any one business, but a foundation for all small businesses to build upon.

Physical Security

This is the layer of security in which we limit physical access to the network. Physical security includes servers, workstations, switches, routers, backup media, etc; essentially anything that has to do with the resources you are protecting.

Previously, we had defined that a threat exploits a vulnerability to access or affect a resource. Therefore, to reduce the risk, we either have to reduce the number or likelihood of threats or reduce the vulnerability. The physical threats and vulnerabilities are numerous. These basic defenses will provide a great deal of security from the multitude of threats.

1. **Provide for physical security for all networking equipment and media**
   - *Locate servers and network equipment in a locked room. Secure equipment to desk or other fixed object.*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

If a device is not locked up, tied down, or otherwise secured, it will be stolen. Even if your business is victim to a break-in, you can protect your data resource by having a secure server room, bolting servers to racks, and locking cases to prevent hot-swap drives from being removed. Laptop and desktop systems can be protected by securing to desks.

- *Secure documentation and media and dispose of properly.*

  Documents and other media (tapes, floppies, zip disk, hard drives, CDs) contain sensitive information that a thief or hacker could use to infiltrate your network. Storage of these items both on-site and off-site must be done in a secure manner. Media safes provide good security and offer protection from fire and heat.

  Shred all discarded network documents including drawings and configuration guides. Used media should also be destroyed.

2. **Provide for protection from equipment failure**
   - *Use redundant equipment on servers.*

     The most common failures in computer equipment are those items with moving parts; namely, hard disk drives and power supply fans.

     RAID (redundant array of inexpensive disk) drive configurations and redundant power supplies should be a requirement on any critical server.

   - *Maintain service contracts on critical equipment.*

     Most small businesses may not be able to justify spare equipment or redundant servers and devices. On-site service contracts can provide security by offering a manageable service window in case of product failure.

3. **Provide protection from environmental threats**
   - *Protect equipment from heat and humidity.*

     Have adequate environmental conditions for your computing equipment. Follow manufacturer requirements for operating environment.

   - *Protect from water damage by not putting servers or UPSs directly on the floor.*

     Placing your servers and UPSs in equipment cabinets or IT shelving can prevent damage from minor flooding, such as a broken water pipe or overflowing toilet.

4. **Provide power protection to servers and network devices**
   - *Install uninterruptible power supplies, UPSs.*

     Power failure can result in data corruption or at a minimum, denial of service. Without electricity, computer equipment doesn't function. UPSs provide protection from short-term power outages and other related power problems such as spikes and sags. Automated shutdown software can also gracefully shut down a server protecting data integrity. It is important to have UPSs not only on the servers, but the network hubs, switches, and workstations as well.

Perimeter / Network Security

This layer of security protects from threats that utilize remote connections to the network. This includes items such as the Internet and remote access devices like phone lines. This differs from the physical security layer in that threats do not have to be physically present

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to cause damage. The threat can often be anonymous, and with the Internet, the threats can be numerous.

For a comparison let's think of the number of people that could pose threats to your environment. If your business is in a city of 200,000 people, then we could say that you have the potential of 200,000 threats. With an Internet connection, this is multiplied nearly 3,000 times to 544 million people.

The common practice in this layer is to deploy a firewall for security. This is a great defense if the firewall is set up properly. A good small-business firewall should have a default configuration blocking all traffic unless specifically allowed. If your firewall works on the premise that everything is allowed unless specifically blocked, buy a new one.

5. **Provide firewall between private network and the Internet**
   - *Install and properly configure a network perimeter firewall.*

     A firewall provides a barrier against disallowed traffic. A properly configured firewall should deny traffic except what is specifically allowed. The access control needs to incorporate both ingress and egress traffic.
   - *Install personal firewall software on systems with dial-up Internet access.*

     Internal systems that dial-up to the Internet become a vulnerability and require personal firewall software. All portable computers should be required to have personal firewall software installed and configured.
6. **Provide security for all Remote Access**
   - *Implement dial-back security for dial-up connections.*

     To provide additional security for a dial-up connection, configure dial-back security. This will only allow remote access from predetermined numbers and prevent an anonymous attack.
   - *Require secure authentication and encryption for VPN remote access.*

     Use MSCHAPv2 for authentication and Point-to-Point Tunneling Protocol (PPTP) to provide for remote access data encryption. For addition security strength, use IPSEC with Layer Two Tunneling Protocol (L2TP).
   - *Log all remote access connections.*

     Configure logging of all remote access connections, both successful and failed. Review the logs on a regular basis and look for unauthorized activity.
7. **Utilize gateway virus protection**
   - *Provide the first layer in virus defense by scanning Internet traffic.*

     Some firewalls (SonicWall, Symantec, and Microsoft ISA Server, to name a few) have virus scanning built in or as an add-on that will scan all Internet traffic and provide the first layer of defense in virus protection.
8. **Utilize secure communication with wireless networking**
   - *Use 128-bit WEP at a minimum for security.*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Most default wireless installations transmit using clear text transmission you would normally find on the wired LAN. Wireless LANs frequently can be accessed from outside the physical security of your environment. At a minimum, 128-bit WEP security should be used. For more security, IPSEC should be used to secure communications on the wireless and wired LAN.

9. Document and know your network

- *Keep documentation of your network current.*

  Having up-to-date documentation of your network is an invaluable resource when you plan, implement, and maintain security. It will also offer assistance to respond to a breach. Auditing your physical network to the documentation may also reveal unauthorized devices that could create security weaknesses.

10. Do not allow the use of P2P file sharing software

- *Remove and disallow use of P2P software such as Napster or gnutella clients.*

  These software applications allow for files on a system to be shared with the Internet, circumventing firewalls and other layers of security. Besides posing a confidential risk, these applications transfer large amounts of data congesting Internet connections to the detriment of legitimate business-related traffic.

Host Security / Operating System Security

A host is defined as any device on your network. This includes servers, workstation, and printers.

11. Use secure operating systems

- *Use only secure operating systems such as Microsoft Windows NT 4.0, 2000, XP, or Linux.*

  The Microsoft Windows 9.x operating systems do not provide a satisfactory minimum level of security. They do not provide for user authentication or file system security. An attacker can bypass authenticating by simply hitting the Esc key, enabling them to have access to the entire contents of the local computer. This poses a threat to the network because the Windows 9.x system maintains a Microsoft password file (.pwd file) that contains the local Windows password that is usually the same as the network password.

12. Strengthen password and account policies

- *Require and enforce strong passwords.*

  Often, this is the last line of defense, or sometimes the only layer of defense. Don't allow easily guessed or dictionary words to be used for passwords. Educate users on password complexity and enforce with Windows 2000 group policies.

- *Implement account policies.*

  Require password changes on a regular interval and do not allow reused passwords. Also, configure account lockout parameters to protect from password guessing.

13. Remove unneeded services and applications

- *Run only needed services and applications.*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The default installation of Microsoft Windows 2000 installs Internet Information Server that includes WWW, FTP, SMTP, NNTP services. If the server is used for basic file and print services, then these IIS services are not required. If left on, they provide another avenue for attack. These extraneous services usually have default settings that do not provide for security and are often overlooked when applying patches.

14. Keep patch levels up-to-date

- *Stay informed on new patch availability.*

  Software companies are releasing fixes to security vulnerabilities on a regular basis. Many offer a notification service to keep you informed. The Microsoft Product Security Notification Service is a great service for those utilizing Microsoft Products http://www.microsoft.com/technet/security/notify.asp. For industrywide notifications try the CERT Advisory Mailing List at http://www.cert.org/contact_cert/certmaillist.html.

- *Install patches.*

  Servers should typically have the patches manually installed and documented. This provides for the best change control and reapplication of patches when necessary.

  Windows workstations user can use the Windows Update Web site at http://windowsupdate.microsoft.com to install critical updates on a regular basis.

15. Remove default accounts and passwords

- *Rename default accounts.*

  Rename the default administrator and guest accounts on Windows NT, 2000, and XP systems. When left as default, an attacker would already know which account names to try leaving just the password to protect you. When the accounts have been renamed, an attacker has to determine both the new account name and password to gain access.

- *Change default or blank passwords.*

  It is never a good idea to have a blank password for any account or device. In addition, many devices come with default passwords that need to be changed. If you implement a firewall but do not change the default password, an attacker would then have access to change the firewall configuration, thus rendering it useless.

16. Install Virus protection and maintain current definitions

- *Use a manageable product that protects servers, workstations, e-mail, and Internet.*

  There is a huge selection of virus protection software on the market. For a business environment, use a manageable product suite such as Trend Micro's NeatSuite or Symantec's Norton Anti-Virus Corporate Edition. These offer central management of virus definitions, deployment, and alerting. From the central console, you can monitor all aspects of your virus defenses.

- *Configure automatic virus definition updates.*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Configure virus definition updates to correspond with the software companies' release dates. Trend Micro, for example, updates their virus definitions weekly on Tuesdays. Symantec offers daily updates.

- *Do not allow end users to disable virus protection.*

  Using the management features of the product, configure the software to not allow the end user to disable or otherwise modify software settings.

17. Have complete backups

- *Create regular backups of critical information.*

  Perform full server backups on a daily basis. This eliminates the confusion often associated with incremental and differential backup strategies. Have a tape rotation scheme that fits your needs with weekly, monthly, or even quarterly cycles.

- *Verify backups are working and test restore procedures.*

  Perform tests on a regular basis to verify that backups are functioning properly and are backing up the correct information. Download basic restore procedures from your backup software company's Web site. Print these out and verify you have the proper information and items to perform a full system recovery. This will include operating system and backup software media, license keys, and server configuration information.

18. Turn on logging and review

- *Log files are an invaluable reference.*

  Reviewing log files on a regular basis can provide information on security breach attempts or unauthorized access. Firewall, Web server, remote access, and other log files can also be used to trace a security breach to validate its occurrence and to what extent damage occurred.

Application Security

The application layer identifies the security of the individual applications that you use on your network. These require much of the same maintenance as do operating systems to reduce technical vulnerabilities. In addition, many end-user errors occur at this level, making accidents or misuse the primary vulnerabilities.

19. Use application authentication when available

- *Make application user names and passwords different from network user names and passwords.*

  Use a different user name and password for application authentication. This can protect an application from inside and outside attacks. Even if an attacker was able to gain access to a valid network account they would not be able to use that same information to access the application.

20. Maintain licensed software

- *Use only licensed software.*

  This is an often overlooked security issue. Allowing unlicensed software can affect both availability and integrity of your resources. Fines can range in the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

tens-to-hundreds of thousands of dollars and injunctions can limit access to your systems and data. These affairs are often highly publicized and detrimental to a business' integrity.

Purchase software only from reputable dealers and retain certificates of authenticity.

21. Patch applications when necessary

- *Applications require security patches, too.*

  New vulnerabilities are found in applications like those in the Microsoft Office Suite that may compromise your network. Install patches to these applications in the same manner as the operating systems patches.

22. Provide sufficient end-user training

- *Train employees appropriately.*

  The biggest threat to network security is usually human error or ignorance. Provide sufficient training so that your staff know what to do if they suspect a security threat. Staff needs to know the security policy and protocols through which the business operates. Periodic testing can be useful to keeping training current.

- *Provide network administrators sufficient training and time to maintain security.*

  Security plans fail when the training and time are not allocated to implement and maintain a security plan. If resources or skills are not available internally, outsource or hire a security consultant to provide sufficient expertise.

Data Security

Protection of the integrity, confidentiality, and availability of the data is at the core of a defense-in-depth strategy. Often, this layer of security is not implemented. This critical component will protect from inside threats.

23. Use file-level security with least-right privileges

- *Give users no more privileges than necessary.*

  By limiting users to the least rights needed to perform their functions, you can protect from vulnerabilities such as accidental file deletion. If users are given read, write, create, and modify rights to the company data directory, they would be able to perform their normal functions and you would protect the data from accidental deletion or drag-and-drop issues. Note: the default configuration of Windows Server gives the Everyone group full control to all files.

- *Implement both share and file/folder permission.*

  A common misconfiguration of user permissions is to assign permission to the share while leaving the folders and files with full control for everyone, or vice-versa. Assign permissions at both the share and file/folder level.

24. Use encryption for highly sensitive data

- *Use Microsoft Encrypting File System (EFS) to encrypt data files.*

  Microsoft's EFS (Encrypting File System) can encrypt directories and files to provide security to highly sensitive information. Use EFS on portable computers to protect their data in case of theft.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CONCLUSION

The small business network is exposed to many of the same security threats as large business but must be able to provide defense with limited resources. It can be done.

Understanding of the key security principles—terminology, risk assessment, defense-in-depth, and policies—provides a common framework for security to be analyzed, implemented, maintained—and most important—of all understood and valued. Following the practical examples will provide a multi-layered security structure to defend your network from a great number of threats by addressing the most important vulnerabilities.

There is no panacea for security. Security is an ever-changing landscape that requires monitoring and adjustment. Reviewing your security plan on a regular basis is a necessity. Stay informed of new vulnerabilities and review your plan and policies at least semi-annually. Knowledge is the first step. You are now knowledgeable, so take action.

References

"Small Business Frequently Asked Questions." 5 April 2002. URL: http://www.sba.gov/advo/stats/sbfaq.html (12 April 2002)

Campbell, June. "Protect your business computer from hackers." 21 February 2000. URL: http://www.fireinternational.com/fire20000221.htm (13 April 2002)

"Security Operations Guide for Windows 2000 Server." 14 March 2002 URL: http://www.microsoft.com/Technet/security/prodtech/windows/windows2000/staysecure/default.asp 30 March 2002

"The SANS Security Policy Project." URL: http://www.sans.org/newlook/resources/policies/policies.htm (12 April 2002)

Nicolls, Weston. "Security is Better in Layers." 16 October 2001 URL: http://www.latimes.com/technology/chi-101016securityblanket.story (12 April 2002)

"80-20 Rule of Information Security." URL: http://securityresponse.symantec.com/avcenter/security/Content/security.articles/fundamentals.of.info.security.html (5 April 2002)

"Defense in Depth Basics." URL: http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html (5 April 2002)

"Corporate Security Policy." URL: http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html (5 April 2002)

Houston, Forrest. "Responsibilities of the "Small Shop" in a Post 11 Sept World." 27 November 2001. URL: http://rr.sans.org/homeoffice/small_shop.php (20 March 2002)

Rasmussen, Scott. "Centralized Network Security Management: Combining Defense In Depth with Manageable Security." 29 January 2002. URL: http://rr.sans.org/practice/central_netsec.php (20 March 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Bayne, James. "An Overview of Threat and Risk Assessment." 22 January 2002. URL: http://rr.sans.org/audit/overview.php (20 March 2002)

Duzenberry, Nate. "The Pursuit of Defense in Depth: Balancing Infromation Security and Business Practices." 28 January 2002. URL: http://rr.sans.org/practice/pursuit.php (20 March 2002)

"The Twenty Most Critical Internet Security Vulnerabilities (Updated)." 8 April 2002. URL: http://www.sans.org/top20.htm (13 April 2002)

"Seven Simple Computer Security Tips for Small Business and Home Computer Users." URL: http://www.nipc.gov/warnings/computertips.htm (20 March 2002)

"Beginner's Guide to Computer Security." The Basics of Computer Security. URL: http://www.staysafeonline.info/beginner.adp (30 March 2002)

"Computer Security Day." URL: http://www.geocities.com/a4csd/how.html (20 March 2002)

"The 7 Top Management Errors that Lead to Computer Security Vulnerabilities." URL: http://www.sans.org/newlook/resources/errors.htm (21 March 2002)

Granger, Sarah. "The Simplest Security: A Guide to Better Password Practices." 12 January 2002. URL: http://online.securityfocus.com/infocus/1537 (20 March 2002)

"Security Tips." URL: http://www.staysafeonline.info/sectips.adp (30 March 2002)

"The Ten Immutable Laws of Security." Microsoft Security Essays. URL: http://www.microsoft.com/technet/columns/security/essays/10imlaws.asp (20 March 2002)

"Information Protection Recommendations." 26 November 2000. URL: http://www.issa.org/awarenessday.html (20 March 2002)

Steinke, Steve. "Tools for Securing Home Networks." 4 March 2002. URL: http://www.networkmagazine.com/article/NMG20020304S0014 (20 March 2002)

Steinke, Steve. "Residential Internet Security." 5 December 2001 URL: http://www.networkmagazine.com/article/NMG20011203S0022 (20 March 2002)

Avolio, Fredrick and Ranum, Marcus. "A Network Perimeter With Secure External Access." February 1994 URL: http://www.avolio.com/netsec.html (10 April 2002)

Belcher, Tim. "Riptech Internet Security Threat Report." January 2002 URL: http://www.riptech.com/pdfs/Security%20Threat%20Report.pdf (23 March 2002)

Power, Richard. "2001 CSI/FBI Computer Crime and Security Survey." Computer Security Issues & Trends. Volume VII, No.1 (Spring 2001): 1-18

Coursey, David. "Cyberterrorists will be after you." 21 February 2002. URL: http://msn.com.com/2102-1107-841889.html (20 March 2002)

"Minimum Data Backup Policy" 24 November 2001. URL: http://www.aub.edu.lb/info/data-backup.html (12 April 2002)

"How Many Online." February 2002. URL: http://www.nua.ie/surveys/how_many_online/ (13 April 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Berg, Al. "P2P, OR NOT P2P?." February 2001. URL: http://www.infosecuritymag.com/articles/february01/cover.shtml (12 April 2002)

"Licenses and Piracy." URL: http://www.asapsoftware.com/eSMART/piracy.htm (14 April 2002)

Symantec Corporation. Security Reference Chart. Poster (April 2001)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.