A decorative graphic on the right side of the page features three overlapping circles of varying sizes, each composed of concentric blue rings. Two thin blue lines intersect at the top left, forming a large 'V' shape that frames the circles.

## **Seven things you need to know about securing your computer network and what you can do to protect yourself**

This article outlines the seven primary security threats a small business should be concerned with and actions that need to be taken to protect yourself.

**ONE Information Technology**

## Table of Contents

<b>1. Protect yourself from within.....</b>	<b>3</b>
<i>Surprisingly enough, there are as many security threats from within as there are from the outside.</i>	
<b>2. Protect yourself from the outside .....</b>	<b>5</b>
<i>Having a firewall and antivirus is not protecting yourself! It is only one piece of the puzzle and needs consistent attention</i>	
<b>3. Keep your data safe.....</b>	<b>7</b>
<i>Your data is difficult to replace.</i>	
<b>4. Protect your Servers from external Attacks.....</b>	<b>9</b>
<i>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.</i>	
<b>5. Perform a Risk Assessment .....</b>	<b>10</b>
<i>A Risk Assessment is a process that helps organizations become more aware of what they have and what is most important to them.</i>	
<b>6. Create a Security Policy.....</b>	<b>11</b>
<i>If you don't already have one, get to work on one. This is an extremely important tool for your organization. It will clearly define how important security is and how far you will go to protect your investments.</i>	
<b>7. Teach Your Employees about Security .....</b>	<b>14</b>
<i>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.</i>	
<b>Appendix - Use strong passwords .....</b>	<b>15</b>

# 1. Protect yourself from within

*Surprisingly enough, there are as many security threats from within as there are from the outside.*

## Physically protect your network

Network security starts with protecting your computer equipment and software as you would any valuable asset. Keep your server in a locked well-ventilated room and limit access to all computers. Get your server off the floor. A burst water pipe could put you out of business. How easy is it for someone to turn off the server by mistake? Keep your backup tapes and disaster recovery tools in a fire proof safe. Don't leave computers logged on to the network for the cleaning staff to access.

## Weak passwords trump strong security – See appendix

The purpose of having a logon process is to establish who you are. Once the operating system knows who you are, it can grant or deny requests for system resources. If a bad guy learns your password, he can log on as if he were you. In fact, as far as the operating system is concerned, he **is** you. Whatever you can do on the system, he can do as well, because he is you. Maybe he wants to read sensitive information you've stored on your computer, like your e-mail. Maybe you have more privileges on the network than he does, and being you will let him do things he normally couldn't. Or maybe he just wants to do something malicious and blame it on you. In any case, it's worth protecting your log on credentials.

Always use a password—it's amazing how many accounts have blank passwords. And choose a complex one. Don't use your dog's name, your anniversary date, or the name of the local football team. And don't use the word "password"! Pick a password that has a mix of upper- and lower-case letters, numbers, punctuation marks, and so forth. Make it as long as possible. And change it often. Once you've picked a strong password, handle it appropriately. Don't write it down. If you absolutely must write it down, at the very least keep it in a safe or a locked drawer—the first thing a bad guy who's hunting for passwords will do is check for a yellow sticky note on the side of your screen, or in the top desk drawer. Don't tell anyone what your password is. We all run into a situation where someone needs a file or rights to perform a job function and you say “just log in as me” As long as that person has your password, the network thinks they are you! Give everyone the rights they need and no more. If you absolutely need to let someone log in as you, change your password as soon as possible afterwards.

## Rogue Administrators

Every computer must have an administrator: someone who can install software, configure the operating system, add and manage user accounts, establish security policies, and handle all the other management tasks associated with keeping a computer up and running. By definition, these tasks require that he have control over the computer. This puts the administrator in a position of unequalled power. An untrustworthy administrator can negate every other security measure you've taken. He can change the permissions on the computer, modify the system security policies, install malicious software, add bogus users, or do any of a million other things. He can subvert virtually any protective measure in the operating system, because he controls it. Worst of all, he can cover his tracks. If you have an untrustworthy administrator, you have absolutely no security.

Even an honest administrator can get rushed and get sloppy.

- ❖ They give out their administrator password to a user as a quick fix when they need access to a program.
- ❖ Forget to disable the account of a fired employee.
- ❖ Run out of time to check the backup tapes.

Often administrators have other duties and managing the network is run off the corner of their desk. They don't have the time or budget for training. The disaster recovery plan and business continuation plan is definitely on the "to do" list.

## What is your staff doing with their computers?

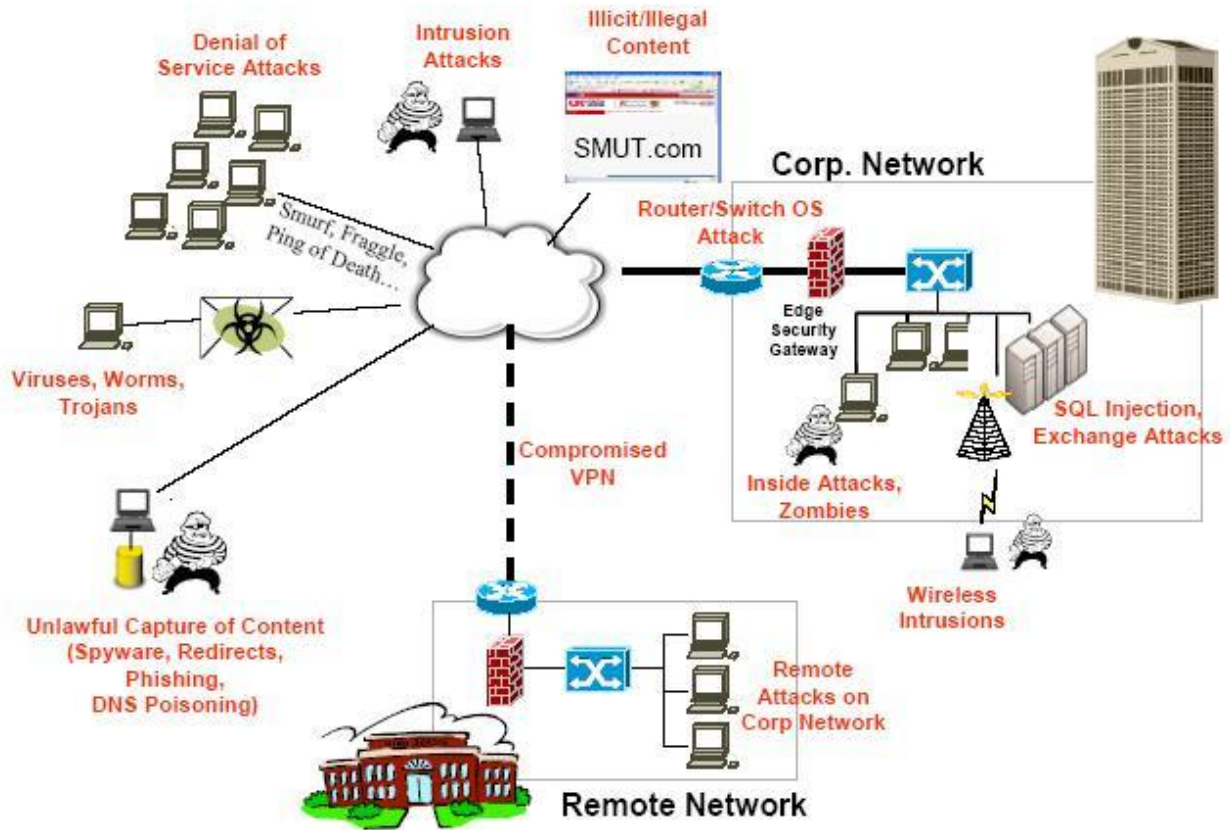
Malicious or by mistake, your own team can bring down the fort. Training is the key solution to this threat. Creating a policy or group of policies for your staff that they can refer to as a guide to using the network is also a good practice.

- E-mail and Internet usage policy
- Streaming Media usage policy
- Instant Messaging
- Etc..

Safe Surfing: Stay away from unscrupulous websites as well as pop-ups and animations. This is a wonderful place to pick up spyware. Casual browsing by employees often opens up a multitude of security threats. Other issues arise from surfing: 70% of online pornography is viewed between 9am and 5pm. Someone passing by and seeing someone's screen may be offended and take legal action against your organization. Online chat and discussion rooms are often frequented by crooks trying to gain information possibly unknowingly from fellow chatters.

## 2. Protect yourself from the outside

*Having a firewall and antivirus is not protecting yourself! It is only one piece of the puzzle and needs consistent attention*



*Figure 1 – Prevalent threat vectors in today's networking environment*

Protect the perimeter layer of your network

- Internet Access
- Email
- Wireless networks
- Branch offices or remote users
- Notebook computers and PDAs
- Floppy discs, CDs, DVDs, USB Flash Drives
- Instant Messaging

The weakest point is where data changes state!

Again - Use Strong Passwords – See appendix

For more information on protecting yourself from the Internet, see our ***“7 things you need to know: Internet Security Threats!”*** white paper or better yet, arrange for a security assessment from ONE Information Technology.

Do NOT under estimate the power of Spyware. It is not just something that slows down your workstation. Spyware can send your client’s credit card information to crooks. It can send your price list to competitors. It can forward your emails to other people. It is a real threat! Do not treat it lightly.

### 3. Keep your data safe

*Your data is difficult to replace.*

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, theft 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 the data on another medium. Set up an automated tape backup process to run every night. You may want to copy all your important files onto a CD(s). For example burn your accounting data onto a CD after each month end is completed. 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 must also keep copies of backups at a secure offsite location.

Keep a backup log and 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. In all current Windows servers—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 a very dangerous practice for maintaining a secure environment—institute a “least privilege” policy by specifically defining user privileges and configuring your servers to give individual users access to specific programs only.

### **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.

Together, these three practices should provide the level of protection most businesses require to keep their data safe.

## 4. Protect your Servers from external Attacks

*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. If you haven't yet taken the steps already outlined in this document, make them a priority. Even if you have already addressed the security measures discussed to this point, you can still do more to protect your servers.

Keep your servers in a safe place.

Keep them up to date. You must install security patches as soon as they become available. Update your hardware and firmware for the server and its accessories such as RAID controllers and tape drives.

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. This 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 security settings you find in Windows Server System products are good only if they are used appropriately and monitored aggressively.

## 5. Perform a Risk Assessment

*A Risk Assessment is a process that helps organizations become more aware of what they have and what is most important to them.*

Ideally, it should identify all information technology assets, to assign a priority rating to each, and to identify threats and vulnerabilities to these assets.

Risk is the possibility that someone or something will either intentionally or unintentionally exploit or attack a computer or system, resulting in damage to that asset. Risk can never be completely eliminated; it can only be mitigated and reduced to an acceptable level. That level will vary according to the importance of an asset to an organization. A Risk Assessment will help a company or organization better understand their risks by weighing the likelihood that an asset will be attacked versus its value versus the cost of protecting it.

### Determining your Assets

An asset is something of value to your organization. In information technology terms, it can be:

- Information and intellectual property
- Computer hardware
- Computer software
- People

Examples of information and intellectual property assets include: customer lists, price lists, supplier details, locally created websites, staff email, company procedures and policies, staff documents and financial records. Computer hardware should include all servers, telecommunications equipment, desktop computers, printers, backup devices and cables. Software assets might include desktop operating systems such as Windows XP; productivity applications such as office suites; server operating systems; and server software. Finally, human assets should never be overlooked.

Once a list of assets has been created they should be assigned a "threat rating" by evaluating them in terms of their importance to the organization's mission.

#### High

Your company would suffer major disruption and legal or financial loss if the asset is attacked. Without this critical asset, your organization would be sufficiently damaged and will no longer be able to fulfill its mission.

#### Medium

Your organization would suffer minor disruption and legal or financial loss if the asset is attacked. Without this important asset, the organization would still be able to fulfill its mission, but in a diminished capacity.

Low

Your organization would suffer no disruption, legal or financial loss if the asset is attacked. Your organization would be able to completely fulfill its mission without this trivial asset.

Computer assets are constantly exposed to threats and vulnerabilities. A threat is a situation in which someone or something deliberately compromises confidentiality, integrity or availability. A vulnerability is a flaw in software code which might be exploited to perform attacks on the networks or computers which use that software. Listing the threats and vulnerabilities of an organization's computers and networks is a vital part of a Risk Assessment.

Finally, it is important that once the Risk Assessment is complete it be put to use. Now that your organization has a clearer idea of what assets it is protecting, it should make decisions on how to protect them. The Risk Assessment merely answers the questions what and why.

## 6. Create a Security Policy

*If you don't already have one, get to work on one. This is an extremely important tool for your organization. It will clearly define how important security is and how far you will go to protect your investments.*

A Security Policy can be one policy or a collection of policies that state what your organization should protect, how it should be protected, how to respond to security threats, and who should be involved in that response.

Creating a Security Policy involves several preliminary steps:

- Create a security team
- Develop usage policy statements
- Review security policies from other similar organizations
- Conduct a risk assessment

A security team should be the group that not only creates the policy but also is responsible for its implementation. Team members should include Management, staff and your IT Support Company (hopefully ONE IT). Ideally, a representative from each department will be included.

There are two broad categories of usage policy statements: statements of the organization's roles and responsibilities and statements concerning users' roles and responsibilities. Some of these statements may be pre-existing, such as a Remote Access Policy, a Password Policy and an Acceptable Use Policy. These can simply be reviewed (and updated if necessary). An Organization's Security Roles and Responsibilities Policy should state what the organization does to protect and maintain resources and why. For instance, the policy could state that the organization provides desktop security measures,

anti-virus software, Internet filtering (or not), and so on. Reasons for these measures should be explained.

Users' roles and responsibilities policies are more numerous. They may include statements such as:

- What is acceptable on the organization's network
- Computers and network are owned by the organization, and that they are provided to the staff for specific, enumerated reasons
- Which laws end users must follow when using the organization's network including:
  - Laws governing use of copyrighted materials
  - Laws governing obscenity and child pornography
- What is NOT allowed:
  - Using email to harass or intimate anyone
  - Running password crackers
  - Installing unlicensed or pirated software
  - Turning on file-sharing
  - Running streaming media applications
- Whether or not the system is monitored
- How the organization enforces the policy; what happens if someone is caught breaking the rules

Whenever possible, review security policies from other similar organizations—after all, why re-invent the wheel?

A Security Policy has the following basic components:

1. Objective or Abstract
2. Scope
3. Responsibilities
4. Physical Security
5. Network Security
6. Software Security
7. Disaster Contingency Plan
8. Acceptable Use Policy
9. Security Awareness
10. Compliance

The Objective should be a mission statement that defines objectives of the policy. It summarizes what types of assets are important, why you need to protect them, and summarizes procedures to be followed to protect these assets. The Scope defines the specific assets to be protected by the policy, based on the Risk Assessment. It also defines who must follow the policy, such as employees, outside contractors, and vendors. The Responsibilities component describes who is responsible for protecting assets defined in the scope, and how. It generally outlines users' security responsibilities, but it can also include roles of particular users, such as IT department managers and administrators.

The Physical Security section states how you will physically protect your facility and assets. It should also state who has access to restricted areas, such as server rooms and telecommunications closets. Network Security states how you will protect data stored on the network. It should include information on:

- Workstation security
- Access control and authentication measures
- File system security
- Backups
- Remote access controls
- Network monitoring
- Port restrictions
- Filtering
- Firewalls, proxy servers and border routers

Software security states how you will use commercial and noncommercial software on servers, network devices and workstations. It describes who is allowed to purchase and install software, who can download from the Internet and how to deal with violators. The Disaster Contingency Plan should cover both hardware and software. (for more information on this, see the ***“7 things you need to know: Disaster Recovery/Business Continuation”*** White Paper). The section on hardware should include a list of equipment to be saved, a detailed hardware inventory with hardware specifications needed for critical assets, a list of the personnel needed to restore servers, and a restore priority. The software section should include information on the software/data backups, off-site storage locations, backup information, personnel needed to restore data, and a restore priority.

An Acceptable Use Policy details the acceptable ways in which the network can be used, including acceptable use of the Internet, emails, acceptable use of computers, limitations on computer use (such as time constraints or filtering restrictions), and sanctions to be imposed if acceptable use standards are not met. Compliance includes details about sanctions to be imposed if the security policy is violated. Sanctions may include:

- Disconnection from network
- Loss of network privileges
- Personnel disciplinary action
- Legal action

Security Policies are not easy to create. They require a lot of effort by many people. Furthermore, they must be constantly reviewed and updated in response to changes in the organization, additional hardware or software, security breaches, new vulnerabilities, and new threats.

## 7. 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.

## Appendix - 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, fingerprints 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. 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
- 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 pass phrase 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).