



# Seven Steps to Help Protect Your Computers

You've made a significant investment in your company's computer systems. They have become necessary for keeping financials, processing orders, taking payments and communication. If anything causes these systems to stop functioning properly, your business can be significantly harmed or even be halted. Don't let this happen.

This guide will help you protect your investment and your business. It will provide you with several basic steps that you can start taking today to protect your company. Use it as a checklist and see where improvements are needed.

## Step 1: Install Software Updates

This is an often ignored, but significant step that you can take to protect a computer. All software has vulnerabilities that can be used by to harm a machine, steal data, or be used for malicious activities. Microsoft, Apple, and other software vendors have added functionality to notify you when something needs to be updated. Listen to these notifications and take the time to apply the updates.

Not all applications that you use will notify you when they need to be updated. And not all of your employees will apply the updates when they are told about them. Make a habit of checking once a month to see what needs to be done.

Here is a list of some common applications that will need patching.

- Windows XP, Vista, Server 2000, Server 2003, Server 2008
- Mac OS X
- Microsoft Office (all versions)
- Firefox Browser
- Adobe Acrobat Reader
- Adobe Flash Player
- Apple QuickTime

- Java
- All Instant Messaging Applications
  - Yahoo IM
  - AOL IM
  - MSN IM
  - Etc

These are just some of the common platforms and applications that are in use in most businesses. You may have graphics applications or other specialty applications. They need the same care.

## Step 2: Use Anti-Virus and Spyware Protection

Anti-virus has been around for a long time now, so most people are used to making sure it is installed on their computer. Anti-virus doesn't catch everything though. Look for an anti-spyware application to use on your systems. A good place to start looking is with the company that creates your anti-virus software. Most anti-virus makers now have spyware detection applications as well. The business versions of these applications usually have a central server that handles updating the computers on your network and providing reports on what is happening.

There is something to keep in mind with these applications. Virus and spyware definition updates are usually provided as a subscription by the vendor. Make sure to include renewing these subscriptions in your budgets. These definitions are updated almost daily so each day that you don't have updated definitions increases the risk of problems. Check weekly (or monthly at the outside) to make sure definitions are being pushed out to your systems. Make sure detected viruses are being cleaned.

## Step 3: Install and Use Firewalls

There are two types of firewalls that you need to be concerned with, software firewalls and network firewalls. A software firewall is installed on the computer directly. Network firewalls are a device that sits at your Internet



connection and watches all traffic entering or leaving your network. They perform similar functions, but are able to handle different situations.

Always make sure to have a network firewall installed. These devices are not a guarantee of safety, but they are essentially a lock on the door. If they are properly installed and configured, they will block all traffic that tries to go through them except for what you specifically allow.

Software firewalls come with Window XP and Vista. Versions of XP before Service Pack 2 do not turn this on by default, so you will need to turn this on. Make **sure** your laptops are using this and that it is not turned off. A laptop may be fairly safe on your company network, but these machines go into bookstores, coffee shops, home networks and other places that you can't control. This will be the first line of defense that a laptop has.

#### **Step 4: Backup Your Data**

This is critical to protecting your data. At first it doesn't look like security issue, but a flood can destroy data as much as anything else. Remember, your data is the core of your business. What will happen if your accounting database gets wiped out?

Invest in a system to backup your data. Things go wrong and mistakes get made. This is your insurance policy that will get you back up and running. Without it, you may find that you don't know exactly who your customers are, what they've ordered, what you charged them or even if you should charge them.

Here are some things that a good backup system and process must do or be:

- **Reliable** - If it isn't getting data saved, then it isn't helping. Reliability is a major consideration.
- **Gets the data out of the building** - A perfectly reliable backup system won't help if the building catches on fire and the tapes are sitting next to the server. Take

them home with you at night if you must, but get them out of the building.

- **Performance** - It has to complete within a reasonable time.
- **Security** - Your data is now on a backup tape and is portable. Keep backup media secure. More systems are offering encryption as they write to media. Take a look at your business needs and regulatory requirements.

These systems are not always inexpensive, so if you don't have a large set of data (greater than 20 GBs or so) consider using an online backup provider. A number of these providers are aware of privacy concerns and have built systems that can meet strict legal requirements. The plus side to using them is that you can install an application on your server, put in your credentials and it starts backing your data up remotely today. This isn't a perfect solution, but if you don't have anything it's a great start.

#### **Step 5: Physical Security**

You can put strong passwords or fingerprint readers on a system, but if someone can get their hands on the hardware they own the computer and its data. Make sure that computer room doors are locked and only specific employees can access them. Create a policy that requires all laptops or removable media to never be left unattended in vehicles, public transportation or other public areas.

If you have particularly sensitive or expensive equipment, look at installing alarms and video surveillance. These are not bulletproof solutions, but they do provide deterrence and the ability to find out if someone did something they should not.

#### **Step 6: Web Proxy Server**

This step might not be too popular with your employees at first, but it really can save you some headaches. A proxy server is a machine that takes all web requests from your employees and proxies them to the web site they are trying to reach. There are several advantages that these devices give you.



- Commercial proxies often provide lists of known “bad” web sites and can prevent access to them. People are frequently victimized when they get sent to a website that hosts malicious software. These devices can prevent an employee from being compromised and hours in clean up being lost.

- You get more control over what your employees are doing during the day. You can figure these applications to block sites based on categories and keep things like adware sites, pornography, streaming video or other undesirable topics off of your network.

- Proxy servers frequently provide caching, which decreases the amount of bandwidth being used and frees it up for other business related traffic.

### **Step 7: Create a Plan**

Perhaps this should be step one, but having a security plan can help you make more consistent decisions regarding computer security. Your plan doesn't have to be large or complex. In fact, when you are getting started simple is better. Try to write it so that it provides practical steps that can be applied to your company. Include things like:

- What is allowed to take place on the network
- What is specifically prohibited from taking place on the network
- Where the anti-virus server is and how to check it to make sure things are up to date
  - How to check if software is up to date and what software should be checked
  - How to make sure the backups are running correctly and how to restore data if needed
  - Specify when you will check these software patches, backups and anti-virus updates to make sure they are working properly.
- What to do if something goes wrong and who will do it
- If you have vendors who provide services for you, include their contact information so that it is readily accessible in an emergency

- Keep it up to date, print it out and keep a copy offsite with your backup tapes. If it is only on the server that just crashed, you could be in trouble

### **Final Thoughts**

Keep in mind that these steps are not meant to cover every thing that may need to be in place. They are meant to provide a foundation that you can use and build on. Your business and technology will change over time; your plan must change with it. Review it at regular intervals and make changes where they are needed. If you feel you need help, find a service provider that you trust who can guide you through the process.

If you've got these steps in place already, congratulations you have taken action on some important things to protect your business. If you see areas where you need improvement, get started on them as soon as possible. Some are more involved than others, but you don't have to have them all done at once. Make a plan to address them and keep moving towards your goal. Make sure your business is safe by taking the necessary steps to protect it.

JW Network Consulting helps businesses keep their computer systems running reliably and securely. If you have questions about this guide or other technology topics, please contact us at 801-326-0364.

For more technology information, visit our website at <http://jwnetworkconsulting.com>