



What Every Small Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

Six Things You Must Do At a Minimum to Protect Your Company from Disaster

*Information, Technology,
Hardware, Software
& Training*

While it's impossible to plan for every potential computer problem or emergency, a little proactive monitoring and maintenance of your network will help you avoid or greatly reduce the impact of the vast majority of computer disasters you could experience.

Unfortunately, we have found that most small business owners are NOT conducting any type of proactive monitoring or maintaining their network, which leaves them completely vulnerable to the types of disasters you just read about. This is primarily for three reasons:

- #1. They don't understand the importance of regular maintenance.
- #2. Even if they DID understand its importance, they simply do not know what maintenance is required or how to do it.
- #3. They are already swamped with more immediate day-to-day fires demanding their attention. If their network is working fine today, it goes to the bottom of the pile of things to worry about. That means no one is watching to make sure the backups are working properly, the virus protection is up-to-date, that critical security patches are being applied, or that the network is "healthy" overall.

While there are over 37 critical checks and maintenance tasks that need to be performed on a daily, weekly, and monthly basis, we're going to share with you the 6 that are most important for protecting your company.

Tech Guides, Inc.
P.O. Box 288
Greenville, WI 54942

920.757.9131

www.techguidesinc.com



Step#1: Make Sure You Are Backing Up Your Files Every Day

It's just amazing how many businesses never back up their computer network. Imagine this: you write the most important piece of information you could ever write on a chalkboard and someone comes along and erases it. How are you going to get it back? You're not. Unless you can remember it, or if **YOU MADE A COPY OF IT**, you can't recover the data. It's gone. That is why it is so important to back up your network. There are a number of things that could cause you to lose data files. If the information on the disk is important to you, make sure you have more than one copy of it.

Step #2: Check Your Backups on a Regular Basis to Make Sure They Are Working Properly

This is another big oversight we see. Many business owners set up some type of backup system, but then never check to make sure it's working properly. It's not uncommon for a system to **APPEAR** to be backing up when in reality, it's not. There are dozens of things that can go wrong and cause your backup to become corrupt and useless. That is why it's not enough to simply back up your system; you have to check it on a regular basis to make sure the data is recoverable in the event of an emergency.

Step #3: Keep an Offsite Copy of Your Backups

What happens if a fire or flood destroys your server **AND** the backup tapes or drive? This is how hurricane Katrina devastated many businesses that have now been forced into bankruptcy. What happens if your office gets robbed and they take **EVERYTHING**? Having an offsite backup is simply a smart way to make sure you can get your business back up and running in a relatively short period of time.

Step #4: Make Sure Your Virus Protection Is ALWAYS On AND Up-To-Date

A virus can be devastating to your network. With virus attacks coming from spam, downloaded data and music files, instant messages, web sites, and e-mails from friends and clients, you cannot afford to be without up-to-date virus protection.

Not only can a virus corrupt your files and bring down your network, but it can also hurt your reputation. If you or one of your employees unknowingly spreads a virus to a customer, or if the virus hijacks your e-mail address book, you're going to make a lot of people very angry.

*Information, Technology,
Hardware, Software
& Training*

Tech Guides, Inc.
P.O. Box 288
Greenville, WI 54942
920.757.9131

www.techguidesinc.com



Step #5: Set Up a Firewall

Small business owners tend to think that because they are “just a small business”, no one would waste time trying to hack in to their network, when nothing could be further from the truth. Studies have shown that it takes on the average less than 12 minutes for a computer with no firewall to be attacked. The simple fact is that there are thousands of unscrupulous individuals out there who think its fun to disable your computer just because they can.

These individuals strike randomly by searching the Internet for open, unprotected ports. As soon as they find one, they will delete files or download huge files that cannot be deleted, shutting down your hard drive. They can also use your computer as a zombie for storing pirated software or sending spam, which will cause your ISP to shut YOU down and prevent you from accessing the Internet or sending and receiving e-mail.

If the malicious programs can't be deleted, you'll have to re-format the entire hard drive causing you to lose every piece of information you've ever owned UNLESS you were backing up your files properly (see 1 to 3 above).

Step #6: Update Your System with Critical Security Patches As They Become Available

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computer through a simple banner ad or through an e-mail attachment.

Not too long ago Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer by tricking users into downloading and opening a maliciously crafted picture. At the same time, Microsoft released a Windows update to correct the vulnerabilities; but if you didn't have a process to ensure you were applying critical updates as soon as they become available, you were completely vulnerable to this attack.

Here's another compelling reason to ensure your network stays up-to-date with the latest security patches...

Most hackers do not discover these security loopholes on their own. Instead, they learn about them when Microsoft (or any other software vendor for that matter) announces the vulnerability and issues an update. That is their cue to spring into action and they immediately go to work to analyze the update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch.

In essence, the time between the release of the update and the release of the exploit that targets the underlying vulnerability is getting shorter every day.

*Information, Technology,
Hardware, Software
& Training*

Tech Guides, Inc.
P.O. Box 288
Greenville, WI 54942
920.757.9131

www.techguidesinc.com



When the “nimda” worm was first discovered back in the fall of 2001, Microsoft had already released the patch that protected against that vulnerability *almost a year before* (331 days). So network administrators had plenty of time to apply the update. Of course, many still hadn’t done so, and the “nimda” worm caused lots of damage. But in the summer of 2003 there were *only 25 days* between the release of the Microsoft update that would have protected against the “blaster” worm and the detection of the worm itself!

How Disaster-Proof Is YOUR Network?

Clearly, *someone* needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible. If you are sitting there thinking, “This all sounds great, but I don’t have the time or the staff to handle all of this work,” we highly recommend small business owners without a full-time IT staff allow their consultant to monitor and maintain their network.

Information, Technology,

Hardware, Software

& Training

The Benefits Are Obvious:

Hopefully this report acted as an eye opener to all small business owners who are not adequately protecting their data and computer network. If you are not doing the 6 steps outlined in this report, your network is an accident waiting to happen and the most important thing for you to do now is take immediate action towards protecting yourself.

One of the biggest, costliest mistakes you can make is to ignore this advice with the false hope that such a disaster could never happen to you.

Tech Guides, Inc.
P.O. Box 288
Greenville, WI 54942

920.757.9131

www.techguidesinc.com

This report has been prepared for you by Tech Guides, Inc. We have been providing computer services in the Fox Valley for businesses with less than 50 computers since 1997. If you have any questions or would like further information please contact us at (920) 757-9131 or e-mail us at dave@techguidesinc.com.