

# The 3 Most *Expensive & Deadly* Computer Disasters That Wipe Out Small Business Owners ... And How To Avoid Them

An Urgent Warning To All Small Business Owners: If You Depend On Your Computer Network To Run Your Business, This Is One Report You DON'T Want To Overlook!

You'll Discover:

- 5 Critical security measures every small business should have in place.
- The single biggest, and costliest mistake most small business owners make when it comes to protecting their irreplaceable company data.
- How to avoid costly network repair bills.
- A simple way to protect your network that won't cost you a dime!

## Have you every lost an hour of work on your computer?

Now imagine if you lost days or weeks of work – or imagine loosing your client database, financial records, and all of the work files your company has ever produced or compiled.

Imagine what would happen if your network went down for days where you couldn't access e-mail or the information on your PC. How frustrating would that be?

What if a major storm, flood, or fire destroyed your office and all of your files? Or if a virus wiped out your server...do you have an emergency recovery plan in place that you feel confident in? How quickly do you think you could recover, if at all?

Many small business owners tend to ignore or forget about taking steps to secure their company's network from these types of catastrophes until disaster strikes. By then it's too late and the damage is done.

After working with hundreds of small and mid-size businesses in Hendersonville, Goodlettsville, Gallatin and the Nashville area, we found that 6 out of 10 businesses will experience some type of major network or technology disaster that will end up costing them between \$4,000 to \$9,000 in repairs and restoration costs *on average*. And that doesn't even include to lost productivity, sales, and client good-will that can be damaged when a company can't operate or fulfill on its promises due to a down network.

What's most exasperating about this situation is that **100% of these disasters and restoration costs could have been completely avoided** easily and inexpensively; and that's why I decided to write this report.

I have found that most small business owners have no idea of the importance of regular preventative maintenance, disaster recovery planning and prevention because 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. Therefore, no one is watching to make sure the back ups are working, the virus protection is up-to-date, or that the network is "healthy".

This is like saying you're too busy driving your car on the highway to put your seatbelt on. Taking that simple preventative step doesn't really show its true value until you get into a head on collision; at that point you are either extremely relieved that you had it on or incredibly sorry that you didn't.

The same holds true with your computer network. Obviously the information on the disk is far more valuable than the disk itself; and if your company depends on having access to the information stored on your server or PC, then it's time to get serious about protecting it from damage or loss.

## Why Small Business Are Especially Vulnerable To These Disasters

With the constant changes to technology and daily development of new threats, it takes a highly-trained technician to maintain even a simple 3-5 person network. But the costs of hiring a full-time IT person are just not feasible for the small business owner.

In an attempt to save money, most try to do their own in-house IT support and designate the person with the most technical expertise as the part-time IT manager. This never works out because this make-shift IT person has another full-time job to do and is usually not skilled enough to properly support an entire computer network anyway.

This inevitably results in a network that is ill-maintained and unstable. It also means that the backups, virus updates, and security patches are not getting timely updates, or may even be set up improperly giving a false sense of security.

It's only a matter of time before the network crashes. If you're lucky, it will only cost you a little downtime.

## **The 5 Most Important Things You Should Do To Make Sure Your Company Is Protected From These Types Of Disasters:**

While it's impossible to plan for every potential computer disaster or emergency, there are a few easy and inexpensive measures you can put into place that will help you avoid the vast majority of computer disasters you could experience.

### **Step#1: Make Sure You Are Backing Up Your System**

It just amazes me 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 chalk board and I come along and erase 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: Perform A Complete Data Restore To Make Sure Your Backups Are Working Properly**

This is another big mistake I 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.

### **Step #3: Keep An Offsite Copy Of Your Backups**

What happens if a fire or flood destroys your server AND the back up tapes or drive? What happens if your office gets robbed and they take EVERYTHING? Having an off-site back up is simply a smart way to make sure you have multiple, redundant copies of your data.

### **Step #4: Make Sure Your Virus Protect Is ALWAYS On And Up-To-Date**

You would have to be living under a rock to not know how devastating a virus can be to your network. With virus attacks coming from spam, downloaded data and music files, web sites, and even e-mails from friends, you cannot afford to not be protected.

Not only can a virus corrupt your files and bring down your network, but it can 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.

## **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; nothing could be further from the truth.

I've conducted experiments where I connected a single computer to the internet with no firewall. Within hours, over 13 gigabytes of space was taken over with malicious code and files that I could not delete. The simple fact is 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 access 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 1-3 above).

## **How Disaster-Proof Is Your Network?**

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 5 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**.