

If Disaster Strikes, How Fast Could Your Company Be Back Up And Running?



You hear it all the time—back up your data, keep your virus protection current, and install and maintain a firewall to protect yourself from hackers and other online threats.

However, while these precautions will certainly help you avoid problems, they CAN'T do anything if you don't have a good backup and disaster recovery plan in place.

We all know that an ounce of prevention is worth a pound of cure; yet, disaster recovery planning often takes a distant second to the daily deadlines and pressures of running a business.

That means that most businesses, including your own, may end up offline and without your data after a simple lightning storm.

Don't think that could ever happen to you? Consider this: "data-erasing disasters" can also take the form of office fires and broken water pipes, not just earthquakes, floods and tornadoes; even more common is software corruption, hardware failures and human error!

Six Things You Must Do To Protect Your Company from These Types of Disasters

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. Here are six steps to a healthy computer network:

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

It just amazes me how many businesses never back up their computer network. Imagine this: you write the most important piece you could ever write on a chalkboard 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. That is why it is so important to back up your network. 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 mistake I see. Many business owners set up some type of backup system, but then never come back 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. 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

You would have to be living under a rock not to know how devastating a virus can be to your network. With virus attacks coming from spyware, 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 email 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 they are "just a small business"; no one would waste time trying to hack into their network, when nothing could be further from the truth. 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; they can 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.

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.

Most hackers do not discover these security loopholes on their own, instead, they learn about them when Microsoft (or any other software vendor) 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. Clearly, someone needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible.

Disaster Recovery Questions You Need to Answer

A disaster recovery plan doesn't have to be complicated, time-consuming or expensive. Start by asking yourself the following questions...

1. Do you back up your company's data daily to both an onsite and offsite location?
2. Are you absolutely certain that your backup copy is valid, complete and not corrupt? How do you know for sure?
3. If disaster strikes, HOW would you get your data back, and how long would it take? In many cases it takes days and often weeks; what would you do during that period of time?
4. Do you have copies of all the software licenses and discs in a safe location that could be accessed in the event of having to rebuild your server?
5. Would you and your employees have a way to access your network remotely if you couldn't get to the office?
6. Do you store important passwords in a secure place that company officers can access if you are unavailable?
7. Do you have a UPS (uninterruptible power supply) device in place to keep your network and other critical data operations running during a power outage?

This is NOT a complete list, but it is a good start to get you thinking in the right direction.

If you are not doing the six critical steps, or cannot answer the seven questions outlined in this article, your network may be an accident waiting to happen. The most important thing for you to do is to take immediate action towards protecting your company.

Michael Mellott, President of XPERTECHS, a local IT Proactive Services firm, can be reached at mmellott@xpertechs.com or 410-884-0225.