

Seven Things You Must Do At A Minimum To Protect Your Company From Common 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.

Unfortunately, I 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. Business owners often rely on the one or two man internal IT staff to ensure that their systems are being properly maintained but have no reporting to verify that work is actually being performed.
4. The vast majority of businesses lack the necessary systems diagnostic tools to monitor and maintain security and performance concerns.
5. Business owners 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.

I'm going to share with you 7 steps that are most important for protecting your company.

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 of information 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. 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 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. 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. Remember the Health Products Company that shelled out \$40,000 to recover data they THOUGHT they backed up? Don't let that happen to you.

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

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, 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.

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. 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 by malicious code and files that I could not delete. The simple fact is that there are thousands of unscrupulous individuals out there who think it's 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 email 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.

Clearly, **someone** needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible. That is why we highly recommend small business owners without a full-time IT staff allow their consultant to monitor and maintain their network.

Step #7: Determine What Maintenance Activities Are Required To Be Performed On Your Network Every Day, Week, And Month, And Monitor To Ensure The Work Is Being Completed.

As I said in the beginning, 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.

With the constant changes to technology and the daily development of new threats, it takes a highly-trained technician to maintain even a simple 5 to 10 person network; however, the cost of hiring a full-time, experienced technician is just not feasible for most small business owners.

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 makeshift 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, giving a false sense of security.

If you can't verify that these seven simple steps have been implemented at your company consider Outsourcing all or part of your IT requirements.

OurTech's Network Management for small and medium sized businesses is offered on a flat rate per device subscription basis. Our flat rate pricing includes device maintenance and unlimited support for a fixed monthly fee; delivering better value than traditional bill-by-the-hour (time & materials) or break fix service models. We help you minimize the hidden costs of PC and server ownership.

The primary benefit to this service model is that it unifies the objectives of OurTech and our clients. OurTech recognizes greater margins when our client's network is operating at peak performance and security and when their employees are well trained on their computing systems. Our clients have the same objective: a well trained staff, efficient technology systems, and enhanced security.

OurTech's Network Management also minimizes the daily hassles involved with using and managing technology, so you can get on with your business. We become an extension of your business, Your IT Department. Our goals include a dramatic reduction in your total cost of technology ownership and a reduction in your technology-induced stress level.

Features

- Flat monthly fee per device
- Technology Vendor Management
- Asset Management
- Strategic Technology Recommendations
- Executive and technical level reporting and accountability
- Includes all components of maintenance, monitoring, and help desk services

Benefits

- Easy to Budget and Predict as you Grow
- Minimize Downtime, Increased Productivity
- Improved Employee morale
- Enterprise class technology tools without the costs
- Operate at best-practices standards
- Have visibility into and receive solid recommendations from IT department
- Give us a call and will give you 15 additional reasons why OurTech is better than your IT Guy.