

Six Things to Do For a Healthy Computer Network

Have you ever lost an hour of work on your computer? Now envision if you lost days or weeks of work – or picture losing your client database, financial records, and all of the work files your company has ever produced or compiled.

What would your reaction be if your network went “down” for days where you couldn’t access email or the information on your server? How frustrating would that be?

What if a major storm or fire destroyed your office and all your files? Or if a virus wiped out your server...a hacker invades your network and steals confidential client information...a disgruntled employee on the way out deletes all your client information and emails/calendar/contacts...workers are streaming songs, video clips, movies, or other content that drains bandwidth, putting the performance of mission-critical applications in peril.

Many SMB owners tend to ignore or forget about the security and health of their computer network – and if they haven’t experienced a major crash, outage or disaster up until now, that’s another item they should put on their list of things to be grateful for this holiday season.

What’s most exasperating about this situation is that 100% of these disasters and restoration costs could have been completely avoided easily and inexpensively with a little planning and proactive maintenance.

So what are the 6 most critical Disaster Proof measures every SMB should have in place?

1. Internet Security

SMB owners tend to think that because of their size, no one would waste time trying to hack into their network, when nothing could be further from the truth. Recently, I conducted an experiment where I connected a computer to the Internet with no firewall. Within hours, over 13GB 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 just waiting to disable your computer. Install a firewall and keep it up-to-date. Add Malware defense by installing Antivirus and Anti-Spyware protection and keep it current. Consider installing an Internet web filtering device that will provide content filtering, application control and bandwidth shaping and prioritization.

2. Email Defense

There are two defenses you must employ to protect your email. The first is SPAM filtering. And this is best done remotely to save costs and reduce the “load” on your server and Internet connection. Find a good hosted SPAM filtering service and let them stop unwanted SPAM before it can reach your server.

The second defense is an email archival system. Why an archival system? Have you ever had an employee leave your company and delete all their email before leaving? Are you concerned about your email storage growing at an annual rate of 35%? Are you faced with legal and regulatory compliance for email retention? Is your Inbox getting too big? Then you need a system that captures ALL in/out-bound email in a secure archive. The benefits are significant and the costs for this type of service are only around \$2/user per month.

3. Data Retention

It just amazes me how many businesses fail to implement procedures to backup their computer network. In fact, most companies that do backup their data do so to a tape device. Yet are you aware that tapes go bad, stretch out and become unusable. The average life expectancy for a tape is 6 – 9 months. Yet most companies continue to use the same tapes for years. In addition to that, tape technology is “old school”. When was the last time you popped in a cassette to listen to your favorite music? The answer to this problem is getting your data off-site through an on-line backup service to a remote facility. The cost for this service has decreased over the past year and is easily affordable (around \$4/GB per month) by all companies. And lastly, create a disaster recovery plan and test it. Make sure you can recover from a disaster before a disaster happens.

4. Patch Management

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computers through a simple banner or through an email attachment. Most hackers do not discover security loopholes on their own. Instead, they learn about them when Microsoft (or any other software vendor like Adobe, Real Player, Flash, etc.) 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.

Similar to patches, hardware manufacturers routinely update their drivers. This includes video cards, sound cards, system boards, firmware on routers and switches, you name it. Some manufacturers have started to release automatic updates for their hardware, but many have not. Make sure you check these sites regularly and when a driver update is available, install it.

With exploits for known vulnerabilities unleashed on the Internet within as little as 5 days from the release of new patches from Microsoft, it is imperative your desktops and servers be regularly updated to keep them safe from attack.

5. Environmental Protection

You’re probably asking yourself what is environmental protection for a network. Well, it is comprised of three factors: The first one is Access Control: Is the network in a locked room? Who has access to the server room? Are your network jacks open to the public and allow unauthorized connectivity? Where are you storing your backups?

The second factor is HVAC: Is your server room cool and do you have adequate ventilation? Does the equipment sit on the floor or is it elevated? Do you have a proactive monitor in place to alert temperature conditions?

The third environmental concern is Electrical: Do you have adequate power in the server room? Are you using dedicated circuits? Do you have a UPS? Is the UPS battery good (average life is 2 years)?

6. Monitoring & Remediation

In today’s world where downtime is not acceptable, it is important for SMBs to know what is going on with the systems on their networks. Proactive monitoring systems can provide user defined alerts 24/7. Receive an alert when a server goes down, users alter their configuration or a possible security threat occurs. These systems provide tools to proactively manage your network and keep the organization running.

Find a help desk organization to provide your end users a central point to receive support on various computer issues, In addition, most helpdesks can utilize remote assistance applications to identify and remediate the problem without the need for on-site support. Most issues can be resolved in 30 minutes or less.

Why Business Owners Must Do These

- Reduce Exposure/Minimize Risk – Protect your entire IT environment from security breaches and leaks.
- Increase Reliability and Predictability – Use proactive monitoring to minimize service outages and reduce the threat of financial loss.
- Control Costs and Complexity – The fastest and easiest way to avoid costly network repair bills while simultaneously making your network run faster. Look for Flat-rate services to allow for effective budgeting.
- Meet Compliance Requirements – Virtually all organizations must satisfy statutory records retention requirements such as the Age Discrimination in Employment Act, Sarbanes-Oxley Act, HIPA, etc.

Isn't it time you took a proactive approach to improve the health of your Computer Network?

Hopefully this article will act as an eye opener to all small and medium business owners who are not adequately protecting their data and computer network. If you are not doing the 6 critical steps outlined in this article, 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.

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