NW Tech Works
Your Technology Team

7 Critical Facts Every Business Owner Must Know About Protecting Their Computer Network From Downtime, Data Loss, Viruses, Hackers and Disasters

If You Depend On Your Computer Network To Run Your Business, This Is One Report You DON'T Want To Overlook!

This report will outline in plain, non-technical English common mistakes that many small business owners make with their computer network that cost them thousands in lost sales, productivity, and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration of these oversights.

You'll Discover:

The single biggest mistake most small business owners make when it comes to protecting their data

7 critical measures to keep data secure

How to greatly reduce – or even completely eliminate – frustrating crashes, slow performance, and other annoying computer problems

How to avoid expensive computer repair bills and get all the computer support you need for a low, fixed monthly rate

How you can eliminate the risk and hassle of tape drive backups while making sure your business can recover quickly from a disruption.

Have you ever lost an hour of work on your computer?

Now imagine if you lost days or weeks of work – or imagine losing 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?

Or, 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.

But That Could Never Happen To Me! (And Other Lies Business Owners Like To Believe About Their Businesses…)

After working with hundreds of small and mid-size businesses across the Chicago 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 $9,000 and $60,000 in repairs and restoration costs *on average*.

That doesn't even include lost productivity, sales, and client goodwill that can be damaged when a company can't operate or fulfill on its promises due to technical problems.

While it may be difficult to determine the actual financial impact computer problems have on your business, you can't deny the fact that they do have a negative effect. If you've ever had your business grind to a screeching halt because your server crashed, you must have some idea of the frustration and financial loss to your business even if you haven't put a pencil to paper in figuring out the exact cost.

Most Computer Problems Are Hidden And Strike Without Warning… At The Most Inconvenient Times

Hardware failure, viruses, spyware, and other problems usually aren't detectable until they strike by causing a server to go down, data to be lost, or some other catastrophe. Viruses and spyware are particularly sneaky because they are designed to hide themselves while they do their damage. For example, spyware can secretly transmit information about you and your company to an outsider without being visible to you.

Even if your network was recently audited by a computer consultant, viruses, spyware, and hackers are constantly attacking your network (that is why we constantly monitor our clients' networks because you never know when a new virus is going to strike).

Unfortunately, most computer consultants only offer "break-fix" services. That basically means when something breaks or stops working, they come in and fix it. While this may seem like a good setup for you, it actually leaves you wide open to a number of threats, problems, and other disasters because it is *reactive* rather than *proactive* maintenance.

Take a look at these statistics:

Companies experience an average of 501 hours of network downtime every year, and the overall downtime costs an average of 3.6% of annual revenue. *(Source: The Costs of Enterprise Downtime, Infonetics Research)*

93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. *(Source: National Archives & Records Administration in Washington.)*

20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. *(Source: Richmond House Group)*

This year, 40% of small to medium businesses that manage their own network and use the Internet for more than e-mail will have their network accessed by a hacker, and more than 50% won't even know they were attacked. *(Source: Gartner Group)*

Of those companies participating in the Contingency Planning & Management Cost of Downtime Survey: 46% said each hour of downtime would cost their companies up to $50,000, 28% said each hour would cost between $51,000 and $250,000, 18% said each hour would cost between $251,000 and $1 million, and 8% said it would cost their companies more than $1million per hour. *(Source: Cost of Downtime Survey Results, 2001.)*

Cyber-criminals stole an average of $900 from each of 3 million Americans in the past year, and that doesn't include the hundreds of thousands of PCs rendered useless by spyware. *(Source: Gartner Group)*

What These Failures Are REALLY Costing Your Business

Set aside the soft costs of lost productivity and consider just the hard cost of repairing and restoring a network. Most major network repairs will require a minimum of four to eight hours to get the network back up and running. Plus, most consultants need a lead time of at least 24 to 48 hours to get on site. That means a downed network could remain out of commission for the better part of a business week.

Even if your network was recently audited by a computer consultant, viruses, spyware, and hackers are constantly attacking your network (that is why we constantly monitor our clients' networks because you never know when a new virus is going to strike).

Unfortunately, most computer consultants only offer "break-fix" services. That basically means when something breaks or stops working, they come in and fix it. While this may seem like a good setup for you, it actually leaves you wide open to a number of threats, problems, and other disasters because it is *reactive* rather than *proactive* maintenance.

Take a look at these statistics:

Companies experience an average of 501 hours of network downtime every year, and the overall downtime costs an average of 3.6% of annual revenue. *(Source: The Costs of Enterprise Downtime, Infonetics Research)*

93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. *(Source: National Archives & Records Administration in Washington.)*

20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. *(Source: Richmond House Group)*

This year, 40% of small to medium businesses that manage their own network and use the Internet for more than e-mail will have their network accessed by a hacker, and more than 50% won't even know they were attacked. *(Source: Gartner Group)*

Of those companies participating in the Contingency Planning & Management Cost of Downtime Survey: 46% said each hour of downtime would cost their companies up to $50,000, 28% said each hour would cost between $51,000 and $250,000, 18% said each hour would cost between $251,000 and $1 million, and 8% said it would cost their companies more than $1million per hour. *(Source: Cost of Downtime Survey Results, 2001.)*

Cyber-criminals stole an average of $900 from each of 3 million Americans in the past year, and that doesn't include the hundreds of thousands of PCs rendered useless by spyware. *(Source: Gartner Group)*

What These Failures Are REALLY Costing Your Business

Set aside the soft costs of lost productivity and consider just the hard cost of repairing and restoring a network. Most major network repairs will require a minimum of four to eight hours to get the network back up and running. Plus, most consultants need a lead time of at least 24 to 48 hours to get on site. That means a downed network could remain out of commission for the better part of a business week.

When the server's hard drive crashed without any warning (since they didn't have anyone monitoring their systems for problems), they lost this entire file. After spending $12,382.57 in costs to not only recover their server back to normal, but also in expensive data recovery fees and lost billings, the firm is, fortunately, back in business.

Left in the lurch. A civil engineering firm hired an IT "guru" to install a new operating system on their server. Instead, the man got them a 6-month trial version and charged them for the license and setup. The operating system was improperly installed to boot, making it a "ticking time bomb" that was about to shut down the network entirely. Amazingly, the company had actually purchased the correct and valid operating system, but it had sat unnoticed on the shelf. After $8,362.75 in recovery and network setup, everything was working properly.

Saved in the nick of time. A local insurance firm had just recently signed up for Dominion's, proactive monitoring and maintenance service from Dominion Computer Consulting. Dominion received early warning signs that one of the hard drives in their server was failing. Thirty minutes later, Dominion received a warning that a second hard drive was failing as well. Within less than an hour of receiving the alerts, Dominion was onsite at the customer's office with a new hard drive ready to save the server from crashing and halting business for several days. The business experienced ZERO downtime that day from a potentially serious problem. What would have happened if Dominion hadn't been monitoring their systems 24/7? Sometime that week, without any warning to anyone at all, the company's server would have crashed and the business would have come to a screeching halt.

Seven Things You Must Do At A Minimum 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. And with proper backups and a disaster recovery plan in place, you'll minimize the risk of downtime and ensure a speedier recovery.

Unfortunately, we have found that most small business owners are NOT conducting any type of proactive monitoring or maintaining their network. Most of them have no plans for how they would recover from a disaster, and trust that their tape backups are all they'll need to get up and running again. Business owners tend to neglect their networks and backups for several reasons:

They don't understand the importance of regular maintenance.

They see the importance of maintenance, but don't know how to do it.

They're swamped by all the other concerns that come with running a small business namely, staying afloat and keeping customers happy.

They think their existing IT provider is "keeping on top of things," while their IT provider is really only there to answer emergency service calls.

They believe their tape backups will be sufficient to restore their system in case of a catastrophic failure. While over 37 critical checks and backup tasks need to be performed on a daily, weekly, and monthly basis, we're going to share with you the 7 that are most important for protecting your company.

Step 1: Set up, install, and configure a business-class firewall.

A firewall is one of the best ways to keep hackers out and data in. Hackers 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, effectively shutting down the hard drive. They can also use vulnerable computers as "zombies" for sending spam, which will eventually cause a company's ISP to shut down its Internet and email access.

At home, many people use their residential routers, such as Linksys or Buffalo wireless stations, as their firewalls – and they assume a similar approach will work for their small business. It won't. Residential solutions don't offer nearly enough security features to effectively secure a business network. You need more than just the firewall that comes with your wireless router; you need multiple lines of defense. Business class firewalls (such as a Cisco PIX) offer the protection that a small business needs to protect the business from easy intrusion. As an extra benefit, these devices allow for the setup of secure VPN, content filtering for the office, and much more.

Step 2: Get business-class virus protection.

With virus attacks coming from spam, downloaded data and music files, instant messages, web sites, and e-mails from friends and clients, small businesses can't afford to be without up-to-date virus protection. A virus won't just corrupt files and bring down a network; it can also hurt a company's reputation. If an employee unknowingly spreads a virus to a customer, or if the virus hijacks the employee's e-mail address book, a lot of people are going to be angry.

Many small business owners believe that personal or free versions of anti-virus software from providers like Norton, Symantec, or AVG will offer adequate virus protection. The fact is that solutions on the low end of the product spectrum, while appropriate for personal

use, just don't offer the functionality you need for business. You need anti-virus software that installs on your Exchange Server and that runs hard drive scans on a regular basis. Free and low-cost solutions won't do that. When it comes to anti-virus software, you get what you pay for. You're much better off upgrading to corporate or business-class editions.

Step 3: Test security patches before you install them to make sure they won't cause more problems than they fix.

Microsoft is notorious for doing a minimal amount of testing on their security patches before releasing them. As a result, security patches may fix old system vulnerabilities but create other issues that cause your system to fail. That's why it's vital to test security patches before you install them – or hire an IT service provider that will do the testing for you, develop a white list of approved patches and a black list of failed patches, and install the white listed patches in a routine, systematic way.

Step 4: Automate your backups.

In many small businesses, one employee has responsibility for performing backups. When that employee is sick, on vacation, or on assignment out of town, those backups might not happen. Or what if the employee simply forgets? Putting your backups on a set, automated schedule significantly reduces the chance of a simple human error putting your whole business at risk.

Step 5: Keep a copy of your backup's offsite.

Many businesses store their backup's onsite, either on a hard drive or a set of tapes. It's handy to have them around in case you need quick access to a deleted or corrupted file – but what happens if some event destroys not only a particular file but your whole physical office? If you only keep a set of backup's onsite, you're one faulty sprinkler system away from disaster. If you keep a full copy of your data someplace far away from your office, your data will still be retrievable even if your building or even your town gets hit by a disaster.

Step 6: Make sure your backups are secure and uncorrupted.

How many times have you read in the paper about some huge business or major government agency losing massive amounts of data because a tape backup was lost in transit or stolen? This is why it's so dangerous to just send backups home with an employee – if that person's car or home is broken into, you could lose your most valuable business asset: your data. We advise using a secure online backup provider who encrypts all transmissions and all stored data.

You should also test your backups quarterly to make sure you can actually perform a full system restore if the occasion ever calls for it. A surprising number of times you'll find that old-media backups, like tape, are corrupted or otherwise unusable.

Step 7: Develop a disaster recovery plan.

Despite all the safeguards you can put in place, sometimes there's no stopping a power outage or natural disaster from seriously compromising your business. That's why it's so important to be prepared with an inventory of all your data and hardware assets, all software license keys, and all vendor contacts so that you can quickly start recovering after a disaster. With a plan in place, you'll know exactly what to do and in what order. Without a plan in place, you're more likely to be stymied by disaster and waste precious time trying to get your business back on line.

Announcing a Simple and Easy Way To

Ensure Disasters Don't Happen To Your Business:

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've got the solution.

Thanks to a service we offer called Marathon, we can completely take over the day-to-day management and maintenance of your computer network and **free you from expensive, frustrating computer problems, downtime, and security threats**. You'll get all the benefits of a highly-trained, full-time IT department at only a fraction of the cost.

And Dominion's secure backup and disaster recovery solution, lets you **safely and automatically upload your financial records, client data, and files right over the Internet to a secure, offsite data center.**

And here is the best part…

In most cases, we can cut your IT support costs by 30% to 50% WHILE improving the reliability and performance of your network; eliminating spyware, spam, downtime, and other computer frustrations; and making sure your business can recover quickly and economically from a disaster.

The Benefits Are Obvious:

You'll eliminate expensive repairs and recovery costs. Our network monitoring and maintenance will save you money by preventing expensive network disasters from ever happening in the first place.

You'll avoid expensive trip fees while receiving faster support. Our remote monitoring software will enable us to access and repair most network problems right from our offices. No more waiting around for an engineer to show up!

How does faster performance, fewer "glitches", and practically zero downtime sound to you? Under this program, that is exactly what we'll deliver. Some parts

Even if your network was recently audited by a computer consultant, viruses, spyware, and hackers are constantly attacking your network (that is why we constantly monitor our clients' networks because you never know when a new virus is going to strike).

Unfortunately, most computer consultants only offer "break-fix" services. That basically means when something breaks or stops working, they come in and fix it. While this may seem like a good setup for you, it actually leaves you wide open to a number of threats, problems, and other disasters because it is *reactive* rather than *proactive* maintenance.

Take a look at these statistics:

Companies experience an average of 501 hours of network downtime every year, and the overall downtime costs an average of 3.6% of annual revenue. *(Source: The Costs of Enterprise Downtime, Infonetics Research)*

93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. *(Source: National Archives & Records Administration in Washington.)*

20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. *(Source: Richmond House Group)*

This year, 40% of small to medium businesses that manage their own network and use the Internet for more than e-mail will have their network accessed by a hacker, and more than 50% won't even know they were attacked. *(Source: Gartner Group)*

Of those companies participating in the Contingency Planning & Management Cost of Downtime Survey: 46% said each hour of downtime would cost their companies up to $50,000, 28% said each hour would cost between $51,000 and $250,000, 18% said each hour would cost between $251,000 and $1 million, and 8% said it would cost their companies more than $1million per hour. *(Source: Cost of Downtime Survey Results, 2001.)*

Cyber-criminals stole an average of $900 from each of 3 million Americans in the past year, and that doesn't include the hundreds of thousands of PCs rendered useless by spyware. *(Source: Gartner Group)*

What These Failures Are REALLY Costing Your Business

Set aside the soft costs of lost productivity and consider just the hard cost of repairing and restoring a network. Most major network repairs will require a minimum of four to eight hours to get the network back up and running. Plus, most consultants need a lead time of at least 24 to 48 hours to get on site. That means a downed network could remain out of commission for the better part of a business week.