



A White Paper from

 **Techcare**™

What Every Small Business Owner Must Know About Protecting and Preserving Their Company's Critical Data and Computer Systems

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.

Edited and contributed to by:
Ross Goldstein
Techcare Practice Area Leader, Network and Communications

ABOUT THE EDITOR

Ross is responsible for the network design and implementation processes enabling Techcare to deliver and support our clients' specific infrastructure needs. These processes also provide a foundation for specialized Techcare solutions.

For the past 18 years, Ross and the Techcare networking team have overseen and implemented networking and communications projects, not only for our clients, but also for some of our clients' customers. Ross' background is highly technical, bringing best practices and state-of-the-art-techniques in delivering services and solutions.



Protecting and Preserving Critical Data and Computer Systems

White Paper Discussion

What Every Small Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

"Do you have an emergency recovery plan in place that you feel confident in?"

What You'll Discover in this White Paper

- The single most expensive mistake most small business owners make when it comes to protecting their company data.
- The universal misconception business owners have about their computer networks, and how it can end up costing between \$9,000 to as much as \$60,000 in damages.
- 6 Critical security measures every small business should have in place.
- 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.



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.

“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.”

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.



Protecting and Preserving Critical Data and Computer Systems

"If you recall the last time you and your employees could not access necessary information, you must have some idea of the frustration and financial loss to your business."

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, professional services firms and Schools in the Chicago area, we found that 6 out of 10 will experience some type of major network or technology disaster. On average, each of these incidents will end up costing them between \$9,000 and \$60,000 in repairs and restoration costs.

That doesn't include lost productivity, sales, and client goodwill that are inevitably 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 have a negative effect. If you recall the last time you and your employees could not access necessary information, you must have some idea of the frustration and financial loss to your business, even if you haven't put a pencil to figuring out the exact cost.



Protecting and Preserving Critical Data and Computer Systems

“20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years.”

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)*



“Most major network repairs will require a minimum of four to eight hours on average to get the network back up and running.”

What These Failures Are REALLY Costing Your Business

Even if you don't factor in the soft costs of lost productivity, there is the hard cost of repairing and restoring your network. Most major network repairs will require a minimum of four to eight hours on average to get the network back up and running. Plus, most consultants cannot get on-site to resolve the problem for 24 to 48 hours. That means your network could be down, at a minimum, for three or more days.

Since the average computer consultant charges over \$150 per hour plus a trip fee and a surcharge if it's an emergency, the average cost of these repairs is \$600 to \$1,000; and that doesn't even include any software or hardware costs that may also be required. Over a year, this results in \$1,800 to \$3,000 in costs without even considering hardware and software costs, or other soft costs of lost sales and work hours. Of course, those numbers quickly multiply with larger, more complex networks.

The worst part for these businesses is that 100% of these disasters and restoration costs could have been completely avoided or greatly mitigated easily and inexpensively with a little planning and proactive maintenance.



"Truthfully, we find that even the best-prepared small businesses will have network problems. It's only a matter of time before the network crashes."

Why Small Business Are Especially Vulnerable To These Disasters

With the constant changes to technology and the daily development of new threats, it can seem like full-time work to maintain even a simple 3 to 5 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 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. We know of at least one company where such an arrangement became a professional hindrance to the job-splitting IT person; he wasn't enthusiastic enough about the IT part of his job to keep the network running smoothly, but the responsibilities kept him from devoting himself completely to his professional duties. In the end, he cost his employer hundreds of thousands in emergency remediation (and he lost both jobs)!

These sorts of half-measures inevitably result in a network that is ill-maintained and unstable. It often means that the backups, virus updates, and security patches are not getting timely updates, while the business owner carries on with a false sense of security, because "he has an IT guy".



Protecting and Preserving Critical Data and Computer Systems

Truthfully, we find that even the best-prepared small businesses will have network problems. It's only a matter of time before the network crashes. If you're prepared, or in lacking preparation, you're extremely lucky, it will only cost you a little downtime; but there's always a chance you could end up like one of these not so lucky examples:

"Vulnerabilities on the workstation side enabled attackers to corrupt those servers; resulting in a remediation project that cost thousands of dollars and weeks of instability"

A High School gets a lesson in network instability

A local High School had recently been through some staff turnover, which brought the predictable confusion while new roles were defined. They called us when workstations throughout the school began slowing down and they discovered major changes had been made to their network directory without the knowledge of any teacher or administrator.

The changes were enough to make several student labs unusable for days. The slowdowns had everyone from teachers to the superintendent beating on the door of the IT office!

As we reviewed the situation with the customer, it became clear that while their servers were in good shape, no one in the new structure had been handling operating system updates or virus definition versions on their workstations.

Even though they'd been up-to-date on their servers, vulnerabilities on the workstation side enabled attackers to corrupt those servers; resulting in a remediation project that cost thousands of dollars and weeks of instability.



Protecting and Preserving Critical Data and Computer Systems

"This client did not want to implement a preventative maintenance program, so the same problem happened again two months later, costing them another \$3,000 and two days of downtime."

Two Failed Hard Drives Cost Health Products Company \$40,000 and 9 Days of Downtime

The back office of a health products company had two hard drives fail at the same time, causing them to lose a large number of critical customer files.

When they contacted us to recover the data from the system backups, we found the backups weren't functioning properly. Even though they appeared to be backing up all of this company's data, they were in fact worthless. In the end, recovering the data off of these failed drives took a team of disaster recovery specialists 9 days and \$15,000. In addition to the recovery costs, they also incurred \$25,000 in other services to get their network stabilized.

Had they been properly monitoring their network, they would have been able to see that these hard drives were failing and that the backups were not performing properly. This would have prevented the crash, the downtime, and the \$40,000 in costs to get them back up and running, not to mention the 9 days of lost productivity while their network was down.

Property Management Company Spends \$9,000 And Weeks Of Downtime For A Simple Inexpensive Repair

A 10-user property management company was not monitoring or maintaining their server. Due to the overuse and lack of maintenance, it started to degenerate and eventually shut down under the load. This caused their entire network to be down for two full days and cost them \$3,000 in support fees to get them back up and running. Naturally the costs were much higher when you factored in the lost productivity of their ten employees during that time.

This client did not want to implement a preventative maintenance program, so the same problem happened again two months later, costing them another \$3,000 and two days of downtime.

Six months later it happened yet another time, bringing their total to \$9,000 in hard costs plus tens of thousands in productivity costs for a problem that could have quickly been detected and prevented from happening.



"Small 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."

Six 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.

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. 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. 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 dozens of critical checks and maintenance tasks that need to be performed on a daily, weekly, and monthly basis, I'm going to share with you the 6 that are most important for protecting your company.



“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#1: Make Sure You Are Backing Up Your Files Every Day

It just amazes me how many businesses aren’t consistently, diligently watching their backups – if they even have appropriate and functioning backups. 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.



“Not only can a virus corrupt your files and bring down your network, but it can also hurt your reputation.”

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.



“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.”

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 computers, using freely available software to hunt down easy marks. 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 without your knowledge as a server 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).



"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."

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.

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.

When the "nimda" worm was first discovered back in the fall of 2001, Microsoft had already released the patch that protected against that vulnerability **almost a year before** (331 days). So network administrators had plenty of time to apply the update. Of course, many still hadn't done so, and the "nimda" worm caused lots of damage. But in the summer of 2003 there were only **25 days**



Protecting and Preserving Critical Data and Computer Systems

"Thanks to a service we offer called Techcare Manage IT 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."

between the release of the Microsoft update that would have protected against the "blaster" worm and the detection of the worm itself!

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.

Announcing A Simple And Easy Way To Ensure These 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," I've got the solution.

Thanks to a service we offer called Techcare Manage IT 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.



Protecting and Preserving Critical Data and Computer Systems

"Our preventative maintenance and network monitoring will make sure your computers stay in tip-top shape for maximum speed, performance, and reliability."

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 of your system will degrade in performance over time, causing them to slow down, hang up, and crash. Our preventative maintenance and network monitoring will make sure your computers stay in tip-top shape for maximum speed, performance, and reliability.
- **You will have ALL of the benefits of an in-house IT department WITHOUT all of the costs.** As a Managed Network Service Plan customer, you'll have access to a knowledgeable support staff that can be reached immediately should you have any kind of problem or question.
- **You'll receive substantial discounts** on IT services that you are already buying. Most IT firms will nickel and dime you over every little thing they do; under this program, you'll pay one flat, affordable rate and get all of the technical support you need. No hidden charges, caveats, or disclaimers.
- **You will never have to fear a big, expensive network repair bill.** Instead, you can budget for network support just like rent or insurance.



Protecting and Preserving Critical Data and Computer Systems

"As a business owner, you already have enough to worry about. We'll make sure everything pertaining to your network security and reliability is handled so you don't have to worry about it."

- **You'll sleep easier** knowing the "gremlins at the gate" are being watched and kept out of your network.
- **You'll safeguard your data.** The data on the hard disk is always more important than the hardware that houses it. If you rely on your computer systems for daily operations, it's time to get serious about protecting your critical, irreplaceable electronic information.
- **You'll finally put a stop to annoying spam, pop-ups, and spyware** taking over your computer and your network.
- **You'll gain incredible peace of mind.** As a business owner, you already have enough to worry about. We'll make sure everything pertaining to your network security and reliability is handled so you don't have to worry about it.

About the Sponsor

Techcare, through a particular focus in continuing care, ensures our customers gain the maximum value from their IT investments through a progressive set of IT outsourcing services.

Techcare assumes accountability for the management of a variety of Information Technology services including server management, security and availability of the infrastructure, end user support and help desk, hardware repair, and responsibility for helping link technology investments to your business plan.

For more information on how Techcare can deliver the results expected from IT, please contact us at info@techcare.com or by calling 847.374.1600.

