GROUP4NETWORKS
"Your Partner For IT Success!"

The 3 Most *Expensive & Deadly* Computer Disasters That Wipe Out Small Business Owners … And How To Avoid Them

An Urgent Warning To All Small Business Owners:
If You Depend On Your Computer Network To Run Your Business, This Is One Report You <u>DON'T</u> Want To Overlook!

You'll Discover:

- **5 Critical security measures every small business should have in place.**

- **The single costliest mistake most small business owners make when it comes to protecting their irreplaceable company data.**

- **How to avoid costly network repair bills.**

- **A simple way to protect your network that won't cost you a dime!**

From the Desk of: Damir Grubisa
President
Group 4 Networks

Dear Colleague,

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

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

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.

After working with many of small and mid-size businesses in the Toronto 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 to $60,000 in repairs and restoration costs *on average*. That doesn't even include lost productivity, sales, and client good-will that can be damaged when a company can't operate or fulfill on its promises due to a down network.

What's most exasperating about this situation is that 100% of these disasters and restoration costs could have been completely avoided easily and inexpensively. That's why I decided to write this report.

I have found that most small business owners have no idea of the importance of regular preventative maintenance and disaster recovery planning because 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. In most cases, no one is watching to make sure the back ups are working, the virus protection is up-to-date, or that the network is "healthy".

This is like saying you're too busy driving your car on the highway to put your seatbelt on. Taking that simple preventative step doesn't really show its true value until you get into a head on collision; at that point you are either extremely relieved that you had it on or incredibly sorry that you didn't.

The same holds true with your computer network. Obviously the information on the disk is far more valuable than the disk itself. If your company depends on having access to the information stored on your server or PC, then it's time to get serious about protecting it from damage or loss.

Why Small Business Are Especially Vulnerable To These Disasters

With the constant changes to technology and daily development of new threats, it takes a highly-trained technician to maintain even a simple 3 to 5 person network. The costs of hiring a full-time IT person are just not feasible for the small business owner.

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 make-shift 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, or may even be set up improperly giving a false sense of security.

It's only a matter of time before the network crashes. If you're lucky, it will only cost you a little downtime; but there's always a chance you could end up like one of these companies:

Auto Body Shop Shells Out $20,000 To Clean Up A Virus

A local auto body shop with multiple locations discovered the importance of preventative maintenance the hard way. Without warning, a virus was downloaded to their server and started replicating and attaching itself to files. This virus corrupted their data, impaired their customer management system, and immediately brought down their Exchange server (no e-mail could come in or go out).

Preventing this disaster would have only cost them $1/25^{th}$ of the cost ($800 per month) AND they would have experienced better performance and fewer problems with their network. Instead, they were forced to spend a whopping $20,000 to remove the virus and restore their network, and that only got them back up and running. Their systems were still not optimized, secured, and updated as they should be.

Two Failed Hard Drives Costs 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 they 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 stable.

Had they been properly monitoring their network, they would have been able to see that these hard drives were failing and that the back ups 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 Down Time 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 support fees to get them back up and running. Naturally the costs were much higher when you factor 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 and tens of thousands in productivity costs for a problem that could have been quickly been detected and prevented from happening.

The 5 Most Important Things You Should Do To Make Sure Your Company Is Protected From These Types Of Disasters:

While it's impossible to plan for every potential computer disaster or emergency, there are a few easy and inexpensive measures you can put into place that will help you avoid the vast majority of computer disasters you could experience.

Step#1: Make Sure You Are Backing Up Your System

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 chalk board 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: Perform A Complete Data Restore To Make Sure Your Backups 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. Remember the Health Products Company that shelled out $40,000 to recover data they THOUGHT they backed up? Don't let this 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? What happens if your office gets robbed and they take EVERYTHING? Having an off-site back up is simply a smart way to make sure you have multiple, redundant copies of your data.

Step #4: Make Sure Your Virus Protect 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, web sites, and even e-mails from friends, you cannot afford to not be protected.

Not only can a virus corrupt your files and bring down your network, but it can 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 were I connected a single computer to the internet with no firewall. Within hours, over 13 gigabytes of space was taken over with malicious code and files that I could not delete. The simple fact is 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. 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 access 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).

How Disaster-Proof Is YOUR Network?
FREE Security Audit Reveals The Truth

Hopefully this report acted as an eye opener to all small business owners who are not adequately protecting their data and computer network. If you are not doing the 5 steps outlined in this report, 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.

<u>One of the biggest, costliest mistakes you can make is to ignore this advice with the false hope that such a disaster could never happen to **you**</u>.

Because you have taken time to request and read this report, I would like to help you make sure your company is safe from harm by offering you a FREE Network Security Audit. Normally we charge $250 for this type of audit, but during this month, I'll make room in my schedule to give away 5 of these to small business owners in Toronto that are concerned about keeping their network and data safe.

During this audit I will come on site and…

- ✓ **Pinpoint any exposure or risk** to potential lapses in security, data backup, power outages, and system downtime.

- ✓ **Review your system backups** to make sure the data CAN be recovered in case of a disaster. You don't want to discover that your back ups were corrupt AFTER a major disaster wiped out your network.

- ✓ **Scan your network for hidden spyware and viruses** that hackers "plant" in your network to steal information, deliver spam, and track your online activities.

- ✓ **Outline a powerful and comprehensive line of defense** against even the most evasive and deadly computer viruses, hackers, and spam for your specific network.

- ✓ **Answer any questions you have** about your network or keeping it running problem free. I can also give you a second opinion on any projects you are considering.

Upon completion of this audit, we'll give you a detailed report in plain English that outlines where you are at high risk for viruses, downtime, or other problems, and discuss what options you have for protecting yourself.

Good Networking,

Damir Grubisa
President
Group 4 Networks
1-866-413-4467
www.g4ns.com

P.S. Please note that this offer for a **FREE Security Audit won't be around forever.** While we would love to be able to give these away to everyone, staff and time limitations simply won't allow it.

That's why we can only give away 5 of these audits during this month on a first come, first served basis (sorry, no exceptions). There are zero obligations for you to do or buy anything when you sign up - so do it now while you're thinking about it!

GROUP4NETWORKS
"Your Partner For IT Success!"

"Yes! I Want To Make Sure My Network And Company's Data Is Safe From Harm"

❑ **Please sign me up for a FREE Security Audit so I can make sure I am doing everything possible to secure my network.** I understand that I am under **no obligation** to do or to buy anything by requesting this audit. I further understand that these audits are being made available on a **first-come, first-served basis**. If I am not one of the first 5, please put me on your stand-by list and notify me if a spot becomes available.

Please Complete And Call:

Name: _____

Title: _____

Company: _____

Address: _____

City: _____ ST: _____ Zip: _____

Phone: _____ Fax: _____

E-mail: _____

Number of PCs: _____

Operating System: _____

Call Me Direct At: 416-523-4137