



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

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 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.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





From the Desk of: David Norris
Managing Director
Nortec IT

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 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!
Although 6 out of 10 Businesses will Experience a Major IT Disaster

After working with over 250 of small, mid-size businesses and infrastructure companies in the Sydney 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 figuring out the exact cost.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





Most Computer Problems Are Hidden And Strike Without Warning, And 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

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





Even if you don't factor in the soft costs of lost productivity, there is a 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 for one to two days.

Since the average computer consultant charges over \$100 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.

What's most exasperating about this situation 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.

I decided to write this report because I have found that most business owners have no idea of the importance of regular preventative maintenance and disaster recovery planning. **Why?** Because they get "Too Busy", they are dealing with the more immediate day to day issues.

Why Small Business Are Especially Vulnerable To These Disasters

With the constant changes to technology and the daily development of new threats, it takes a highly-trained technician 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 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.

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:

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





Direct Marketing Company Shells Out \$12,000 To Clean Up A Virus

A multinational direct marketing company 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 a fraction 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 \$8,000 to remove the virus and restore their network. Even then, this huge enormous fee only got them back up and running; their systems were still not optimized, secured, and updated, as they should have been.

We then put in place process and equipment to stop this happening again. This included a firewall with Anti-Virus scanning built in.

Two Failed Hard Drives Cost Real Estate Company \$45,000 and 5 Days of Downtime

The back office of a large Real Estate 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. The backup software used was incompatible with the tape technology and was incorrectly reporting success. In the end, recovering the data off of these failed drives took a team of disaster recovery specialists 10 days and \$15,000. In addition to the recovery costs, they also incurred \$15,000 in other services to get their network rebuilt. And an additional \$15,000 for a new HP Server to replace their white box unbranded server.

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 \$45,000 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.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





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.

Five 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 over 105 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.

Threat #1: Make Sure You Are Backing Up Your Files Every Day and taking them Offsite

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.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





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 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.

Prevention : Make sure you have a backup process in place. This should be a two pronged solution. Onsite and Offsite. There are a couple of solutions or combinations of solutions that can be used.

Tapes are still the most effective – but are also the most costly. Tapes allow you the benefit of having both onsite and offsite backups over a period of time, by using a combination of daily's, weekly's and monthly's.

USB Drive backups: We can now fully image your server onto a USB hard drive. This can be restored to any other server in a matter of hours. A USB drive can be taken offsite weekly or daily.

Internet Based backups : These are a fantastic solution for data only based backups, but are not practical for server backups. This is primarily because of large file sizes generated daily.

Threat #2: Check Your Backups On A Regular Basis To Make Sure They Are Working

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.

Prevention : 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 Real Estate Company that shelled out \$40,000 to recover data they THOUGHT they backed up? Don't let that happen to you.

Threat #3: 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.

Prevention : Ensure you have a corporate antivirus installed on your network. The free ones are not up to the task and have too many limitations. This needs to be monitored and maintained daily. If the Virus patterns are out of date or the program has been disabled then your network is at risk. WE normally deploy and enterprise class product that is fully monitored and managed by us with prices starting at \$60 per device per year.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





Step #4: Not Having 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.

Prevention : A Router or modem with NAT inbuilt is not suitable for a business firewall. Firewalls now can do the following at the gateway

- Antivirus
- Antispyware
- Intrusion Prevention
- Monitoring
- Reporting
- Black and White lists.

Better to stop the problem at the Gate than at the Front Door.

We use Sonicwall Firewall devices, to keep our client secure.

Step #5: 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...

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





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** 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.

Prevention : All of Nortec’s support plans including the monitoring and applying of patches.

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, “Hassel Free 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.

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 and eliminating spyware, spam, downtime, and other computer frustrations!

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





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.
- **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.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





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.

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**.

Because you have taken the time to request and read this report, I would like to offer you a FREE Network Security Audit.

During this audit I will come on site and...

- ✓ **Pinpoint any exposure to or risk** from hackers, viruses, spyware, spam, data loss, power outages, system downtime, and even employee sabotage.
- ✓ **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 backups 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.
- ✓ **Look for hidden problems that cause error messages, slow performance, and network crashes.**
- ✓ **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.

**There Are No Strings Attached,
But You Have To Hurry...**

As you might have guessed, I cannot extend this offer forever, because time and staff limitations simply won't allow it.

If you want to say goodbye to your computer problems and stop worrying about the security of your data from hardware failures, viruses, hackers, and other threats, then you'll want to sign up right now for this Free Network Security Audit.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





There is absolutely no obligation or pressure for you to buy anything, or to ever use our services again. As I stated earlier, this is simply an easy way for us to demonstrate how we can help your business at no risk to you.

How To Secure Your Free Network Security Audit

1. Fill in and fax back the enclosed request form.
2. Call me direct on 02 9894 9514
3. Send an e-mail to sales@nortec.com.au with the words, "Security Audit" in the subject line. Be sure to include your company name, address, and phone number so I can follow up with you.

Good Networking,

David Norris
Managing Director
Nortec IT
02 9894 9514
www.nortec.com.au

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 you must respond to this offer by the date stamped on the enclosed fax-back form today.

You have my word that you will not be under any pressure or obligation to buy anything, or to ever use our services again.

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





“Yes! I Want To Make Sure My Network And Company’s Data Are 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.

Please Complete And Fax Back:

Name: _____

Title: _____

Company: _____

Address: _____

City: _____ Post code _____

Phone: _____ Fax: _____

E-mail: _____

Number of PCs: _____

Fax To: 02 9899 8125

Call Me Direct At: 02 9875 3353

44/5 Anella Avenue (PO Box 431), Castle Hill NSW 2154
Phone: (02) 9894 9514 Fax: (02) 9899 8125
Email: sales@nortec.com.au Website: www.nortec.com.au





Here's What Are Clients Are Saying About Us:

"every year we have an exercise where Nortec executes our DR plan and to get our staff and part of the operations centre up and running again"... "This years exercise was done within 24 hours and we had a 100% success rate"

Operations Manager of a Major Sydney Infrastructure Company

"Tresco steel has been dealing with Nortec for 8 years. It has proved to be a successful business relationship. WE have constantly found the staff at Nortec to be friendly and reliable. Their knowledge and advise is instrumental in the efficient running of our network"

AT Nicholl – Group Commercial Manager – Tresco Steel Pty Ltd

"We have found them to be extremely responsive and effective at dealing with issues that we might have relating to our IT requirements. This includes the setting up of communications technology, as well as recommendations on solutions for improved efficiency in the workplace, and the cost effective supply of computer equipment"

Rob Hardy (Managing Director) - Time Life Australia P/L

"Nortec has always advised our company appropriately for all of our business needs and they are very effective in saving us money on our IT needs"

Kristin Jorgensin (Company Director) - TriFlex Electrical