



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.



Dominion Computer Consulting

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.



Dominion Computer Consulting

Furthermore, there's the cost of consulting. The average computer consultant charges over \$100 per hour plus a trip fee and a surcharge if it's an emergency, so the average cost of these repairs is \$600 to \$1,000 – excluding software or hardware costs that may also be incurred. Over a year, these results in \$1,800 to \$3,000 in service costs, plus the cost of hardware, software, lost sales, and diminished productivity. And those numbers quickly multiply with larger, more complex networks.

There is a silver lining, however: disasters and restoration costs can be easily and inexpensively mitigated, if not avoided altogether, with a little planning and proactive maintenance.

Do Any Of These Scenarios Describe Your Small Business?

Technology is constantly evolving – and so are threats. As a result, it can take a highly trained technician to effectively maintain even a simple 3 to 5 person network. However, the cost of a full-time, experienced technician is well outside the budget of most small business owners.

Most small businesses resort to one of two options. They either designate the employee with the most technical expertise as the unofficial IT manager – leaving that person frustrated, overworked, and often out of their depth when it comes to technology – or they outsource IT to independent “computer gurus” who, in spite of the description, generally lack the experience, the expertise, and the resources to really support small business clients.

In-house employees and outsourced “gurus” might be able to put out the occasional fire or perform routine “break-fix” work. But they don't have partnerships with tech industry leaders that will give them the best pricing on hardware and software. They can't provide round-the-clock emergency support. And they don't have the infrastructure to host remote backups or perform remote monitoring and maintenance.

As a result, small businesses too often have networks that are ill-maintained, unstable, and out of date when it comes to backups, virus updates, security patches, and licenses.

It's only a matter of time before the network crashes. And for a small business, a little bit of downtime can make a huge impact on the bottom line. Here are a few real-life examples taken from Dominion Computer Consulting customers to show the threats they faced before they started taking a proactive approach to IT:

The not-so-safe, not so-secure data backup. A local accountant faithfully backed up its data on a regular basis. They even took those backups offsite every week and thought that everything was working great. There was just one problem: someone in the office had taken the business' most critical file – the one that held all of the firm's time and billing information -- and had de-selected it from the backup routine due to space constraints.



Dominion Computer Consulting

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:



Dominion Computer Consulting

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.



Dominion Computer Consulting

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



Dominion Computer Consulting

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 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, and your data is being backed up automatically to a secure remote location.

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.

You'll have your data backed up automatically right over the Internet. No more rotating and storing tapes – one more important item off your to-do list!

You're not limited to the size of your tape drive. You can back up ALL of your data and applications so that you can fully restore your system.

With our Managed Network Service Plan Gold and Platinum packages, even a complete disaster won't keep you down for long. If a disruption occurs, you will have access to a full working copy of your server (including all applications) in 48 hours or less – no waiting for days or even weeks for your data and then having to re-install all your applications and databases like other solutions require!



How Disaster-Proof Is YOUR Network?

FREE Backup 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 7 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 read this report, we would like to offer you a FREE Backup Audit. Normally we charge \$300 for this service, but as a prospective client, we would like to give it to you for free as a way of introducing **Dominion's Service Plan Gold and Platinum packages** to your company.

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

Audit your current data protection including backup and restore procedures, tape rotations and maintenance schedule to see if there is anything jeopardizing your data's security.

Review procedures for storage and transportation of data. Many people don't realize they damage their disks (and thereby corrupt their data) by improperly caring for their storage devices.

Check your network backups to make sure they are accurately backing up all of the critical files and information you would NEVER want to lose.

Talk about the makeup of your data, including the age and type of files you are backing up. Why should you care? Because many companies inadvertently use valuable computer storage to back up their employees' personal MP3 files and movies.

Discuss current data protection needs and explain in plain English where your risks are. We know everyone has a different level of risk tolerance, and we want to make sure all the risks you're taking with your data are by choice not because of miscommunication or accident.



Why Do We Give This \$300 Service Away For FREE?

Unlike most quick-fix computer guys, we flat-out refuse to simply put a band-aid on your problem and then leave you wide open to future problems and disasters. If all you want is a cheap fix that will get you through to the end of the day, *then please contact someone else.*

What we'll do is immediately fix your most urgent problem—guaranteed—to at least get you back up and running. But we won't stop there...

After we've got your system stable, we'll conduct a thorough Computer Security and Vulnerability Audit to uncover hidden problems such as spyware, viruses, security loopholes, unstable hardware, corrupt software, spam gateways, and other conflicts that will cause your system to frequently crash and run slow. We'll also check to make certain your backups are working properly.

Why Should You Care About This?

Because there are at least 5 ways hackers and viruses can access your network—undetected—to embezzle your private information, steal your identity, and use your network as a conduit for spreading spam, viruses, and even illegal software.

There are numerous system checks and updates that should be done on a regular basis to ensure maximum speed, performance, and security. Ignore them and your system will get progressively slower, unstable, and susceptible to viruses, spyware, and hackers.

Tape backups have a failure rate of 100% - that means all tape drives will fail at some point, without warning. You don't want to find out that your backup was not working the day after your hard drive was erased.

That Recurring “Glitch” Could be a Sign of a Much Deeper Problem Developing

Your present emergency – or even a recurring glitch, slow performance, or other strange behavior - could be a sign of a much deeper problem developing. That's why we offer this audit to all new clients. In no time at all we can assess your network – while you watch – and show you what's really going on 'under the hood' so you can take appropriate action to protect yourself.



Dominion Computer Consulting

Look for incorrect network configurations that show up as unexpected down time, application errors, printers not working, and e-mail problems.

Pinpoint productivity bottlenecks that are causing you to miss client deadlines and frustrate your employees.

Assess your risk to potential lapses in security, data backup, power outages, and system downtime and **outline a powerful and comprehensive line of defense** against even the most evasive and deadly computer viruses, hackers, and spam.

Other Companies Have Paid Over \$300 for This Service

But it's yours FREE Just for Giving Us a Chance

We've decided to give you this free Backup Audit as a gift so you can put us to the test without committing to anything.

While we don't expect everyone to hire us to monitor and maintain their network, we know that a good majority of you will become life-long clients like these loyal customers:

How to Take Your First Step to a More Secure, Reliable, and Headache-FREE Computer Network

To schedule your FREE Backup Audit, simply give us a call at (800) 296-2203 or send in the completed fax back form found at the end of this document.

We'll respond immediately to answer any questions you have and to schedule a convenient time for a senior technician to come on site.

P.S. When you sign up for your Free Backup Audit you will be under **no obligation to hire us for anything** – so call us right now while you're thinking about it



Dominion Computer Consulting

Please Complete This Form:
Your Name & Title:
Company:
Address:
City, State, Zip:
Phone:
E-mail Address:
Number of PCs:
<p style="text-align: center;">Please contact me immediately! I have a project or a problem I need your help with.</p>