The 7 Most *Expensive & Deadly* Backup Mistakes That Wipe Out Businesses… And How to Avoid Them

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?

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 hundreds of businesses in the Washington, DC area, we found that more than half will experience some type of major network or technology disaster. We have seen these types of disasters end up costing between $9,000 to $60,000 in repairs and restoration costs. That doesn't even include the hidden costs of 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; and that's why I decided to write this report.

I have found that most business owners have no idea of the importance of regular preventative maintenance, disaster recovery planning and prevention 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. Therefore, 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; and 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 to Mid-Sized Businesses Are Most 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 five person network. The costs of hiring a full-time IT person are just not feasible for many businesses.

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:

Two Failed Hard Drives Costs Local Real Estate Developer $10,000 and 9 Days of Downtime

The back office of a real estate development company had two hard drives on a server fail at the same time causing them to lose a large number of critical company files.

When they contacted us to recover the data from the system backups, we found they weren't functioning properly and 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 cost thousands of dollars. In addition to the recovery costs, they also incurred thousands of dollars in other services to get their network working again.

Had they been properly backing up their server and monitoring the backups, 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 thousands in costs to get them back up and running, not to mention the 9 days of lost productivity while their network was down.

The 7 Biggest Backup & Disaster Recovery Mistakes Most Companies Make:

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 backup related disasters you could experience.

#1: Not Backing Up Your Systems

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.

#2: Not Monitoring and Verifying Your Backups Are Working Properly

This is another big mistake we see. Many business owners set up some type of backup system, but then never verify 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 Real Estate Development Company that shelled out thousands to recover data? They had someone on their staff watching these backups and THOUGHT they were working. Your backups need to be monitored regularly by a professional to ensure they are working.

#3: Not Having 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? How much would this cost your company? Could your company survive? Having an off-site back up is simply a smart way to make sure you have multiple, redundant copies of your data.

#4: Letting Someone on Your Staff to Manage the Backups

If I only had a nickel for every time this happens: The business owner designates the most technical person on their staff to manage the backups. This person backs up the data to

a hard drive, tapes, or an online service, but doesn't have the IT expertise to understand whether the backups are complete or truly working. Eventually a hard drive fails or a system crashes and they discover the backups are garbage and spend thousands with us recovering.

We can tell you with confidence that backups are difficult to manage, even for us. We use only the best backup software and have staff of highly trained system engineers watching them around the clock and we still run into challenges. Ask yourself, if it is this hard for us, how is your secretary going to effectively handle them?

#5: Trusting Cheap/Bargain Online Backup Services

I am sure you have seen and heard the advertisements "Backup all of your music and files for only $49.00 a year." These services are fine for home use, but are ill-equipped to backup critical server data, databases, email archives, and company files. We could tell you many horror stories about these backups failing, but we challenge you to do a simple Google search for "xyz online backup restore failure." You will find thousands of accounts of failed backups yourself. The unfortunate truth is there is no such thing as a cheap or bargain backup service. Trust us, if there were, we would be using it to back up our own data. No business should put their valuable data in the hands of one of these services.

#6: Using Tape Backups

Tapes are without a doubt the most unreliable form of backups. Take the Google search challenge again. Lookup "tape backup failure rate" and be prepared for your jaw to hit the floor. Many experts say that tapes fail up to 70% of the time. Not a very reliable form of backup. You should never trust your data to a tape backup.

#7: Bad/Cheap IT Advice

Bad IT advice is the root of a lot major backup and network problems. There are ton of part time IT experts out there and IT people you can pay by the hour to work as needed. Not all technicians are created equal. Just because a person is good with computers or run an IT business on the side does NOT mean they know or understand backups and servers in depth. It also does Not mean they have the hundreds of thousands of dollars in backend software and infrastructure necessary to monitor and verify backup integrity.

Most business owners/CEOs look for a part time "IT guru" to help them to save money. This approach always comes back to haunt them. We get customers all the time who need us to clean up a backup mess that was caused by an inexperienced "guru". True IT professionals do not work cheap. They are either just getting started or have no idea what they are doing. All it takes is one mistake with a backup to cost your business everything.

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

Hopefully this report acted as an eye opener. If any of the seven areas outlined sound like you, your backups are an accident waiting to happen.

<u>One of the biggest, costliest mistakes you can make is to ignore these trouble areas 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, we would like to help you make sure your company is safe from harm by offering you a FREE Network Evaluation.

During this evaluation we 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 and are being backed up properly.

- ✓ **Scan your network for hidden problems** that lie dormant waiting to cause a problem.

- ✓ **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.

Contact us today to schedule a time:

703-264-7776

sales@networkdepot.com