Connectability

What Every Business Owner Must Know About Hiring An Honest, Competent, Responsive And Fairly Priced Computer Consultant

Don't Trust Your Company's Critical Data And Operations To Just Anyone!

21 Revealing Questions You Should Ask Any Computer Consultant Before Giving Them Access to Your Company's Network

Dedicated To Your Success

info@connectability.com | 647-930-2250

CONSUMER CHOICE AWARD 2024 GREATER TORONTO AREA 7 YEAR WINNER

"12 Little-Known Facts and Insider Secrets *Every* Business Owner Should Know About Data Backup And Disaster Recovery"

If your data is important to your business and you cannot afford to have your operations halted for days – even weeks – due to data loss or corruption, then you need to read this report and act on the information shared. This report will outline the most commonly made, costly mistakes that most small business owners make with their data backups.

You'll Discover:

- What remote, offsite, or managed backups are, and why EVERY business should have them in place.
- 7 critical characteristics you should absolutely demand from any offsite backup service; do NOT trust your data to anyone who does not meet these criteria.
- Where hard drive and tape backups fail and give you a false sense of security.
- Frightening trends, cases, and questions every business owner should know and consider regarding data security.
- The single most important thing to look for in an offsite backup service provider.

Provided By: Connectability
Author: Brad Shafran, President
www.connectability.com
647-930-2250
970 Lawrence Ave W, Suite 402, Toronto

From the Desk of: Brad Shafran

President
Connectability

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 and you couldn't access email or the information on your PC. How devastating 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?

If you do not have good answers to the above questions, or a rock-solid disaster recovery plan in place, you are quite literally playing Russian roulette with your business. With the number of threats constantly growing, it's not a matter of *if* you will have a problem, but rather a matter of *when*.

But That Could Never Happen To Me!

(And Other Lies Business Owners Like To Believe About Their Businesses…)

After working with over 500 small and mid-size businesses in the Toronto area over the past 25 years, we've 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 data loss would have on your business, you can't deny the fact that it would have a major negative effect on you, your employees, and your clients.

"But I Already Back Up My Data," You Say…

If you are like most business owners, you've been smart enough to set up some kind of backup – possibly hard drive, or even tape backups. But know this:

The average failure rate for a tape backup is 100% - ALL tape backups fail at some point in time.

Incredible, isn't it? Most people don't realize that ALL tape drives fail. But what's really dangerous is that most companies don't *realize* it happened until it's too late.

That's why history is riddled with stories of companies losing millions of dollars worth of data. In almost every case, these businesses had some type of backup system in place, but were sickened to find out it wasn't working when they needed it most.

Disk (USB) Backups aren't much better!

USB drives are certainly cheaper, more common place, and they hold more information than tape drives. But all you have to do is accidentally drop that drive, and all your data is gone. And if you never take it offsite, it won't protect you from fires, floods, theft or vandalism.

And here's the other thing: most companies who do disk backup, write their backups onto the same drive, over and over again! What happens if you need to recover a file from a few months or even a few weeks ago? It's gone forever.

While you should maintain a local backup of your data, neither tape nor disk backups will offer you protection if…

1. Your tape drive malfunctions rendering it useless and making it impossible to restore your data. IMPORTANT: It is *very* common for a tape drive to malfunction without giving any warning signs.

2. Your disk drive is dropped or otherwise broken.

3. Your office (and everything in it) gets destroyed by a fire, flood, hurricane, tornado, or other natural disaster.

4. The physical tapes or hard drives you are backing your data up to become corrupted due to heat or mishandling.

5. A virus spoils the data stored on the drive. Some of the more aggressive viruses not only corrupt the data, but they don't allow anyone to access the data on the drive.

6. Someone in your office accidentally wipes the tape or disk, erasing everything on it.

7. Theft – a disgruntled employee intentionally erases everything, or a thief breaks in and steals ALL of your equipment.

8. A faulty sprinkler system "waters" all of your electronic equipment.

Bottom line: You do NOT want to find out your backup was not working when you need it most.

Frightening Trends, Cases, and Questions You Should Consider:

- Tape drives fail on average 100% of the time; that means ALL tape drives fail at some point and do NOT offer complete protection for your data if a natural disaster, or fire destroys your office and everything in it. Business owners who were hit by hurricanes like Katrina learned a hard lesson about keeping offsite backups of their data.

- 93% of companies that lost their data for 10 days or more 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 email will have their network accessed by a hacker, and more than 50% won't even know they were attacked. *(Source: Gartner Group)*

- About 70% of business people have experienced (or will experience) data loss due to accidental deletion, disk or system failure, viruses, fire or some other disaster (*Source: Carbonite, an online backup service*)

- The first reaction of employees who lose their data is to try to recover the lost data themselves by using recovery software or either restarting or unplugging their computer — steps that can make later data recovery impossible. (*Source: 2005 global survey by Minneapolis-based Ontrack Data Recovery*)

Offsite Backups: What They Are And Why EVERY Business Should Have Them In Place

The ONLY way to completely protect your data and guarantee that you could restore it all after a major disaster is by maintaining an up-to-date copy of your data offsite in a high-security facility.

Remote backups, also called offsite backups, online backups, cloud backups or managed backups, is a service that allows you to maintain a secure copy of your data in a different location than your office.

Usually this type of backup is done automatically via the Internet to a high-security facility. There is no question that every business owner should have an offsite copy of their data; however, there ARE big differences among offsite backup services and it's critical that you choose a good provider or you could end up paying a lot of money only to discover that recovering your data – the very reason why you set up offsite backups in the first place – is not an easy, fast, or simple job.

7 Critical Characteristics to Demand from Your Remote Backup Service

The biggest danger businesses have with offsite backup services is lack of knowledge of what to look for.

There are literally hundreds of companies offering this service because they see it as an easy way to make a quick buck. But not all service providers are created equal and you absolutely want to make sure you choose a good, reliable vendor or you'll get burned with hidden fees, unexpected "gotchas," or with the horrible discovery that your data wasn't actually backed up properly, leaving you high and dry when you need it most.

If your offsite backup provider doesn't meet all 7 of these points, then you'd be crazy to trust them to store your data:

1. **Military-level security, data transfer, and data storage**. This is fairly obvious; you want to make sure the company housing your data is actually secure. After all, we are talking about your financial information, client data, and other sensitive information about your company. Never trust your data to anyone that doesn't have the following security measures in place:

    a. Ask your service provider if they are PIPEDA, PHIPA, and OSC compliant. These are government regulations that dictate how organizations with highly sensitive data handle, store, and transfer their data. If you are a medical or financial institution, you are required by law to work only with vendors who meet these stringent requirements. But even if you are NOT an organization that falls under one of these regulations, you still want to choose a provider who is because it's a good sign that they have high-level security measures in place.

    b. Make sure the physical location where the data is stored is secure. Ask your service provider if they have an ID system, video surveillance, security guards, and some type of key card system to allow only authorized personnel to enter the site.

    c. Make sure the data transfer is encrypted with SSL protocols to prevent a hacker from accessing the data while it's being transferred.

2. **Multiple data centers that are geographically dispersed**. Anyone versed in data security knows the best way to avoid loss is to build redundancy into your operations. All that means is that your offsite backup service should store multiple copies of your data in more than one location. That way, if a terrorist attack or natural disaster destroys one of *their* locations, they have

backups of your backup in a different city where the disaster did not strike.

3. **Ideally, you should have** the ability to recover from a serious failure within hours – not days. If you're using a consumer-grade backup solution like Dropbox or Carbonite, you'll be totally dependent on Internet download speeds to get your data back. An effective backup provider should offer you options like complete image backups, booting your server in the cloud or even complete business continuity and disaster recovery. They cost a little more, but if you experience a disaster, you'll be glad you have them.

4. **Ensure that your backup provider offers sufficient backup history, ideally infinite.** The last thing you want is to go to your backup, only to find that the document you want to restore is the same as the version you already have. An effective backup provider should allow you to "roll back" to any date, so you can retrieve the version of the data that you need.

5. **Make sure your data can be restored to a different computer than the one it was backed up from**. Amazingly, some backups can only be restored to the same computer they came from. If the original computer was burned in a fire, lost, stolen, or destroyed in a flood, you're left without a backup.

6. **Demand regular status reports of your backup**. All backup services should send you a weekly or monthly email to verify your backup actually ran AND to report failures or problems. The more professional providers should also allow you to notify more than one person (like a technician or your IT person) in addition to yourself.

7. **Demand help from a qualified technician**. Many online backup services are "self-serve." This allows them to provide a cheaper service to you. BUT if you don't set your system to back up correctly, the money you will save will be insignificant compared to the losses you'll suffer. At the very least, ask your service provider to walk you through the steps on the phone or to check your settings to make sure you did the setup properly.

The Single Most Important Thing To Look For When Choosing an Offsite Backup Service Provider

While the above checks are important, one of the most critical characteristics – and one that is often overlooked -- is finding a company that will do regular test restores to check your backup and make sure the data is able to be recovered.

You do not want to wait until your data has been wiped out to test your backup; yet that is exactly what most people do – and they pay for it dearly.

If your data is very sensitive and you cannot afford to lose it, then test restores should be done monthly. If your situation is a little less critical, then quarterly test restores are sufficient.

Any number of things can cause your backup to become corrupt. By testing it monthly, you'll sleep a lot easier at night knowing you have a good, solid copy of your data available in the event of an unforeseen disaster or emergency.

And if you work with an IT Provider or MSP, they should be monitoring your backups on a daily basis to ensure that backups are being done successfully.

Want To Know For Sure If Your Data Backup Is Truly Keeping Your Data Secure?

Our Free Data Security Analysis Will Reveal the Truth…

As a prospective new client, I'd like to extend a "get to know us" offer of a Free Data Security Audit. I don't normally give away free services at Connectability because if I did, I'd go out of business. But since your company meets our strict selection criteria, I thought this would be a great way to introduce our services to a few new clients.

At no charge, a security specialist will come on site and…

- Audit your current data protection including backup and restore procedures, hard drive 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 hard drives and tapes (and thereby corrupt their data) by improperly caring for their storage devices.

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

- 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.

Depending on what we discover, we'll either give you a clean bill of health or reveal gaps in your data backup that could prove disastrous. If it's appropriate, we'll provide you with an action plan for further securing your data with our Business Continuity backup solution.

Naturally, I don't expect everyone to become a client, but I do expect a small percentage to hire us to protect their most valuable asset--corporate data--and possibly even become loyal clients.

But I Don't Need a Free Security Analysis Because My IT Guy Has it Covered…

Maybe you don't feel as though you have an urgent problem that needs to be fixed immediately. Maybe you think your data is perfectly safe. Many of our current clients felt their data was safe until it became necessary for them to RESTORE THEIR DATA.

Unfortunately, that is when most companies "test" their data backup and restore solution. We are helping companies like yours AVOID embarrassing and extremely costly data catastrophes like these:

> Despite receiving regular warnings that their tape backups were operating unreliably, a Toronto area company ignored those warnings (and ours) until the day they needed to restore the mailbox of a former employee. That employee was suspected of pilfering thousands of dollars from the company's coffers.
>
> Unfortunately, because their backups were not functioning correctly, they were NEVER able to restore that mailbox and as a result, they were unable to recover any of the stolen funds.

Here is yet another…

Another client of ours learned their lesson the hard way, which is all too often the case. They insisted on performing hard drive backups instead of offsite backups because they thought it would save them money. Their solution was to save their files over and over again onto the same hard drive.

One day, they discovered that they had been infected with **Ransomware**, and all of their files were encrypted and unusable. And because they only had a **single** disk backup, they had no way of recovering from the infection.

Eventually, they had to go to an old backup and re-enter **6 weeks** of work. Sure, offsite backup would have cost them a bit more, but the hours of lost productivity outweigh that cost 10-fold.

Why Trust Your Offsite Backups To Us?

There are a lot of companies offering offsite backup services, so what makes us so special? Why choose us over the dozens of other companies offering what appear to be the same services? I'm glad you asked because there are 5 BIG reasons to trust us with your data security:

1. All of the solutions we use have state of the art facilities protected by 24-hour security, biometric access and perimeter fencing and patrols. All of the sensitive electronic equipment is fully redundant with backup power and generators and multiple connections to the Internet. Plus, they have multiple data centers, so even if one burns down, your data is still protected.

2. We offer free help desk support for recovering files. Some companies charge you extra for this service, or don't offer it at all.

3. We offer free disaster recovery services to restore your data if ALL of it is lost at one time. Again, most companies charge extra for this, or they don't offer it at all. At no additional charge, we will work directly with your IT manager or network support consultant to get all of your data restored in the unfortunate event of a catastrophic loss.

4. We are a local company with a real, live office. That might not seem too unique to you, but what you don't realize is that some offsite data companies are made up of a couple of guys working from their back bedrooms with no way of actually reaching them other than by email or phone.

We'll come on site, shake your hand, and buy you a cup of coffee. Wouldn't you rather deal with a local company that can meet with you face to face rather than an unknown entity in a different province – or different country?

5. We will conduct monthly or quarterly test restores of your data (depending on your support plan) to truly determine if your backup is working. There is no other way of knowing for sure and MOST offsite backup services do NOT offer this service.

But Don't Take Our Word for It – Just Look What Our Clients Have to Say…

"Proactive, Reliable IT Support That Nonprofits Can Trust"

We are a small, nonprofit arts service organization and Connectability's IT support services have been of great benefit to our team. They are responsive to our needs, and we always feel comfortable reaching out because we know Connectability will be prompt and helpful in providing an effective solution. They are also proactive in identifying potential areas of improvement and suggesting IT solutions before major issues arise. Their team is professional, reliable and knowledgeable in all areas of IT support. We highly recommend their services.

Diane Davy Executive Director
Work in Culture

"Their Responsive Local IT Support Keeps our Manufacturing Operations Running Smoothly"

As a small business, we don't have the resources for a full-time IT staff, so having Connectability by our side has been a game-changer. Their team provides responsive and professional technical support exactly when we need it, without the overhead. Since we specialize in manufacturing, it's crucial for our operations to stay uninterrupted, and Connectability's local support is always available. They consistently deliver with quick response times and on-site support whenever needed. I'd absolutely recommend them for the value, service quality, and peace of mind they bring."

Scott Jones General Manager
KB Components Toronto Inc.

"Connectability is A Trusted IT Partner That Feels Like Part of Our Own Team"

Since Connectability took over our IT, the biggest benefit has been their responsiveness. Working with them feels like having an extension of our own team—someone who not only knows what they're doing but also guides us through challenges with confidence and expertise. What sets Connectability apart is their proactive approach to minimizing risk. They don't just react to issues; they help prevent them before they occur. Their efforts to educate our team, like weekly cybersecurity emails and simulated phishing tests, have been invaluable in reducing risks and improving our overall security. We've worked with other IT firms in the past, but Connectability is the best fit by far. Their combination of proactive guidance, effective issue resolution, and day-to-day responsiveness makes them an exceptional partner for any business.

Brian Leon CEO
Choice Hotels Canada

"In our experience of working with Connectability, we have found them to be unfailingly honest, responsive and reliable"

That level of trust has really given me the peace of mind that our IT operations are being taken care of effectively. I also feel like they really have our best interest in mind – something you don't get from every IT provider. If you have any doubts, I recommend reaching out to their CEO Ted and scheduling a call!

Michael Elman CEO
Plastic Dress-Up Inc