



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

“12 Little-Known Facts and Insider Secrets *Every* Business Owner Should Know About Backing Up Their Data and Choosing a Remote Backup Service”

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 remote backup service; do NOT trust your data to anyone who does not meet these criteria.
- Where 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 a remote backup service provider.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com



**From the Desk of:
Joseph Stoll
President
Technical Action Group Inc.**

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 e-mail 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 everything was stolen? Or a virus wiped out your server? Or a disgruntled employee erased all of your data...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 50 small and mid-size businesses in the Greater 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 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.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

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.

“But I Already Back Up My Data,” You Say...

If you are like most business owners, you've been smart enough to set up a tape or hard drive backup. But know this:

The average failure rate for tape and hard drive backups is 100% - ALL tape and hard drive backups fail at some point in time.

Incredible, isn't it? Most people don't realize that ALL tape and hard 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.

While you should maintain a local backup of your data, a tape backup will NOT offer you protection if...

1. Your tape/hard drive malfunctions rendering it useless and making it impossible to restore your data.
IMPORTANT: It is *very* common for a tape/hard drive to malfunction without giving any warning signs.
2. Your office (and everything in it) gets destroyed by a fire or flood or other natural disaster.
3. The physical tapes/drives you are backing your data up to become corrupted due to heat or mishandling.
4. A virus spoils the data stored on the tape/hard drive. Some of the more aggressive viruses not only corrupt the data, but they don't allow anyone to access the data on the tape/drive.
5. Someone in your office accidentally formats the tape/drive, erasing everything on it.
6. Theft – a disgruntled employee intentionally erases everything, or a thief breaks in and steals ALL of your equipment.
7. 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.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

Frightening Trends, Cases, and Questions You Should Consider:

- Tape/hard drives fail on average at 100%; that means ALL tape/hard drives fail at some point and do NOT offer complete protection for your data if a fire, or flood destroys your office and everything in it or a thief steals your server. Business owners who lost everything in the Queen Street fires in February 2008 learned a hard lesson about keeping remote 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 e-mail 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*)

Remote 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, 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 after hours 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 remote backup services and it's critical that you choose a good provider or you could end up



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

paying a lot of money only to discover that recovering your data – the very reason why you set up remote 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 remote backup services is lack of knowledge in what to look for.

There are dozens 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 remote 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 data is encrypted before it leaves your servers with an encryption key that only they have. The data should then be encrypted again for its transit over the internet. Files should be stored, in encrypted form, on multiple servers in high security facilities. Each file should be encrypted using 256-bit AES encryption technology. This means the encrypted data cannot be read without the corresponding keys, so encrypted data cannot be misused, even if it's stolen.
 - b. Make sure the physical location where the data is stored is secure with access to authorized personnel only. Ask your service provider if they have an ID system, video surveillance, and some type of card key system to allow only authorized personnel to enter the site.
- 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 remote 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. Demand that there's an alternative method to retrieving your company's data (in the event of a loss) other than downloading from the internet.** If your entire network gets wiped out, you do NOT



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

want Internet download to be your only option for recovering the data because it could take days or weeks. Therefore, you should only work with a remote backup provider that has an alternative method to provide your data, other than by internet download.

- 4. On that same token, ask your service provider if you have the option of having your *initial* backup performed through hard copy.** Again, trying to transfer that amount of data online could take days or weeks. If you have a large amount of data to backup, it would be faster and more convenient to send it to them on hard drive.
- 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, stolen, or destroyed in a flood, you're left without a backup.
- 6. Demand that the backup system is being monitored 24/7 x 365.** Your remote backup service provider should be monitoring your remote backups 24/7 x 365 so that they are notified immediately upon any failures or problems, and they can address them right away.
- 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.

The Single Most Important Thing To Look For When Choosing a Remote 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.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

Why Trust Your Remote Backups To Us?

There are a lot of companies offering remote 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? There are 7 BIG reasons to trust us with your data security:

1. **Your business can be back up and running within TWO hours of a server crash or failure. With all of your data in tact. This is HUGE!** A dedicated backup server is installed in your office so that if your main server crashes, the backup server can take the place of your main server and in as little as TWO HOURS, we can have your business back up and running, with all of your data, while your server is being repaired or replaced. No worries – the server is included in the affordable monthly fee for the service, so you don't pay thousands up front for the server.
2. **Your data is as secure as Fort Knox.** Data is encrypted before it leaves your servers with an encryption key that only we have. The data is then encrypted again for its transit over the internet. Files are then stored, in encrypted form, on multiple servers in high security facilities. Each file is encrypted using 256-bit AES encryption technology. This means the encrypted data cannot be read without the corresponding keys, so encrypted data cannot be misused, even if it's stolen.
3. **Your data is mirrored in two data centers** – one on the east coast and the other on the west coast for additional redundancy and security. This means that if one center is affected by a disaster (fire, flood) then your data is safe and secure in the other, unaffected location.
4. **The backup server is monitored 24/7 x 365** to ensure your data is being backed up.
5. **Each month we will conduct a test recovery** on sample data to make sure the system is working. There is no other way of knowing for sure and MOST remote backup services do NOT offer this service.
6. **If one of your staff intentionally or unintentionally deletes files, we've got you covered.** Data is quickly restored from the backup server located on your premises. It's possible to recover a file that was modified in the past 15 minutes! This is not possible with a tape or hard drive backup system.
7. **If your main AND backup servers are destroyed by fire or flood, or stolen** a new backup server containing the most recent backed up data from the off-site backup centre would be delivered to you and installed within 3 business days if the event happens during the week, or 5 days if on a weekend.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

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 Technical Action Group because if I did, I'd go out of business. But since you took the time to request and read this report, I thought this would be a great way to introduce our services to a few new clients. **Our only criteria to qualify for this offer is that your company has at least one Windows server and 10 Windows workstations.**

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

- Audit your current data protection including backup and restore procedures, tape/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 tapes/disks (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.
- Present a simple and easy to understand chart that will detail 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 music.
- 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 TAGuard Backup and Disaster Recovery Service for Small Business.

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.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

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:

The President of a Marketing firm based in Toronto thought their data was backed up safe and sound each night. After all, he had an IT guy that was responsible and spent thousands of dollars on the appropriate tape solution and purchased highly regarded software to run it all. So as you can imagine, he was upset when he was told their server crashed and they needed to restore it from tape.

Flash forward three weeks, **\$62,000 and a BRAND NEW IT PERSON later**, and they restored as close to "before failure" as possible (much of the data was lost forever so best guesses were taken). According to the President, who understandably asked to remain anonymous, the worst part of the whole experience is thinking you are doing all the right things spending money on solutions that APPEAR to be working when, in reality, they aren't.

And here's another....

Another client of ours learned their lesson the hard way, which is all too often the case. The tape backup appeared to be working, but when he needed it most, it failed to restore. They had to recreate almost a month's worth of data because the tape failed. In the Director of IT's own words, "I had my bags packed and was ready to be shown the door. The only reason I have my job today is because I proved to my boss that all indications were the data was being backed up. All the logs and reports noted backup and verify completed without errors. The tape just didn't work.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

You are Under No Obligation to Do or Buy Anything When You Say “Yes” to a Free Data Security Analysis

We want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our offer.

As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

However, I cannot extend an unlimited number of these offers every month because time and staff limitations simply won't allow it. Each month, I do up to 5 of these free audits. In order to secure your Free Data Security Analysis for your company as soon as possible, call me while you're thinking about it. Spots ARE limited to 5 each month so act today so you don't have to go on a waiting list.

To schedule the analysis, do one of the following:

1. Call me (Joe Stoll) immediately at 416-489-6312 x 204
2. Complete and fax back the attached form
3. E-mail to Info@TechnicalActionGroup.com and put “Free Data Security Analysis” in the subject line.

Sincerely,

Joseph Stoll
President
JStoll@TechnicalActionGroup.com
Direct Line: 416-489-6312 x 204

PS: A friendly reminder that to qualify for this free analysis, your company must have at least one Windows server and 10 Windows workstations.



Facts About Backups

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

“Yes! Sign me up for a Free Data Security Analysis so I can know for sure that my data will be there when I need it most!” Please reserve one of your FREE Data Security Analyses in my name. I understand that I am under no obligation to do or to buy anything by requesting this free service.

My company has at least one Windows server and 10 workstations.

At no charge, we will send a data security specialist to your office to:

- ✓ 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 backup system to make sure it is accurately backing up all of the critical files and information you would NEVER want to lose.
- ✓ Present a simple and easy to understand chart that will detail 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 music.
- ✓ 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.

Please Complete and Fax Back:

Name: _____
Title: _____
Company: _____
Address: _____
City: _____ Prov: _____ PC: _____
Phone: _____ Fax: _____
E-mail: _____

Fax This Form To: 416-778-1714