"12 Little-Known Facts and Insider Secrets *Every* Business Owner and Organization Leader Should Know About Backing Up Their Data and Choosing An Offsite Backup Service"

If your data is important to your business or organization and you cannot afford to have your operations halted for days – even weeks – due to data loss, corruption, or being held in a ransomware attack 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 businesses and organizations make with their data backups.

You'll Discover:

- What offsite and on-premise backups are and why EVERY small and mid-sized business and organization 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 backups fail and give you a false sense of security.
- Frightening trends, cases, and questions every business owner and organization leader should know and consider regarding data security.
- The single most important thing to look for in and offsite backup service provider.

From the Desk of: Timothy D. Ricketts

President, T. Daniels Consulting

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 organization has ever produced or compiled.

Imagine what would happen if your onsite network went down for days and you couldn't access e-mail (if located onsite) or critical client or business data. 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 or you are the victim of a cyber attack like ransomware and all of you are literally locked out of all of your files…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 (DR) plan in place, you are quite literally playing Russian roulette with your business or organization. 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 and Organization Leaders Like To Believe About Their Businesses…)

After working with hundreds of small and mid-size businesses and organizations in the area, we have found that 6 out of 10 of these types of organizations 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 they 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 or organization, 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 or organization leaders, you've been smart enough to set up a backup. But know this:

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

Incredible, isn't it? Most people don't realize that scheduled backups fail. But what's really dangerous is that most owners and leaders don't *realize* it happened until it's too late.

That's why history is riddled with stories of companies and organizations losing millions of dollars worth of data. In almost every case, they 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, that backup will NOT offer you protection if…

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

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

3. The physical backup device (portable hard drive, CD, USB flash drive, etc.) you are backing your data up to become corrupted due to a laundry list of reasons.

4. A virus or cyber attack spoils the data stored on the backup device. Some of the more aggressive viruses not only corrupt the data, but they don't allow anyone to access the data on the drive. And in case you were not aware, ALL ransomware attacks encrypt the data files, making them inaccessible, and demands a ransom payment to decrypt them.

5. Someone in your office accidentally formats the backup device, 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.

Frightening Trends, Cases, And Questions You Should Consider:

- Backup jobs fail on average at 100%; that means ALL backup devices fail at some point and do NOT offer complete protection for your data if a natural disaster, fire, or terrorist attack destroys your office and everything in it. Business owners and organization leaders who were hit by hurricanes like Harvey and Michael learned a hard lesson about keeping offsite backups of their data.

- Nearly 72% of small and mid-sized businesses and organizations experience cyber-attacks and half do not know how to protect their companies. *(Source: Ponemon Institute's 2020 State of Cybersecurity in Small and Medium Size Businesses.)*

- 93% of businesses 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 and mid-sized businesses and organizations will suffer a major disaster causing loss of critical data every 5 years. *(Source: Richmond House Group)*

- 40% of small and mid-sized businesses and organizations 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 organizations have experienced (or will experience) data loss due to accidental deletion, disk or system failure, viruses, fire or some other disaster (*Source: CompTIA*)

- The first reaction of employees who lose 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: global survey by Minneapolis-based Ontrack Data Recovery*)

Offsite Backups: What They Are And Why EVERY Business and Organization 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.

Offsite backup 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 scheduled and completed automatically via the Internet. There is no question that every business owner and organization leader should have an offsite copy of their data; however, there ARE big differences among offsite backup providers 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 An Offsite Backup Provider

The biggest danger you have with offsite backup services is lack of knowledge in 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 organization Never trust your data to anyone that doesn't have the following security measures in place:

a. Ask your service provider if they are HIPAA, Sarbanes-Oxley, GLBA, and SEC NASD compliant. These are government regulations that dictate how organizations with highly sensitive data (like banks and doctor's offices) 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 and meets, at a minimum SSAE-18 and FIPS 140-2 certification standards.

c. Make sure the data transfer is protected with military-level 256-bit AES encryption.

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 cloud 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 the ability to receive secure, overnight copies of your data if needed.** If your entire network gets wiped out, you do NOT 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 cloud backup provider that will provide overnight copies of your data via a secure physical storage device.

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 via a secure device.

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 or destroyed in a flood, you're left without a backup.

6. **Demand daily status reports of your backup.** All backup services should send you a daily e-mail to verify if 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 offsite 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 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.

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

Our Free Data Backup And Security Assessment Will Reveal The Truth

If you are worried about whether or not your current backup and security processes are up to par, I'd like to give you a Free Data and Cyber Security Assessment ($895 value) as a means for introducing our services to you. Why do we do this? Simply because I know how confusing and difficult it can be to find a good IT support company that is responsive, easy to work with and actually knows what they're doing.

Just about anyone can say they are an "IT expert." And since most business owners and organization leaders don't have the ability to evaluate whether or not their IT company or person is doing a good job, we find that offering this free service is a great, no-risk way of demonstrating how we can help you. At the very least, you'll get a free, 3rd party evaluation of your current backup, which is extremely valuable even if you don't choose to hire us.

At no charge, one of our security specialists will come on site and…

- Audit your current data security and protection, including backup and restore procedures, tape drives or other onsite backup devices to validate if all of your data is actually being backed up in a format that could quickly be restored. (We often discover data on drives, laptops or PCs that is overlooked.)

- Discuss how long it would take you to be back up and running in the event of an emergency or server crash based on your current system.

- Assess if your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees. If you're not getting weekly security updates from your current IT person, your systems probably aren't secure. You should also know that antivirus software and most firewalls are grossly inadequate against the sophisticated attacks now happening.

- Answer any questions you have about backing up and securing your data. We're also happy to put together two or three options for backup and security based on your specific needs and budget. 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 Gold Care Managed Backup service.

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 like Swartz Ambulance (backing up 6 servers, all HIPPA compliant) or Spring Meadows Country Club (backing up 2 servers, including PCI compliance).

But I Don't Need A Backup And Security Audit 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 that 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 organizations like yours AVOID embarrassing and extremely costly data catastrophes like these:

The President of a Flint based manufacturing and robotics company 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 backup 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 backup.

Flash forward three weeks, **$28,000 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.

Another client of ours learned their lesson the hard way, which is all too often the case. The 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 backup 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 backup just didn't work. **Since starting with Gold Care Managed Backup, I get test restores regularly because it's so easy and they ALWAYS confirm if they work**."

How To Request Your Data Backup And Security Assessment

To request this, simply do one of the following:

1. Call our office at 810-629-0131
2. Send us an e-mail to info@tdaniels.com
3. Go online to https://www.tdaniels.com/backup-assessment/

As soon as we receive your request, we'll call to schedule a convenient time for us to meet with you and to conduct the audit of your backup system. Again, you are under no obligation to do or buy anything. Even if you choose not to hire us for any additional work, you'll at least get a free, 3rd party evaluation of your company's data backup and security.

Why Trust 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? I'm glad you asked because there are 6 BIG reasons to trust us with your data security:

✓ Our state-of-the-art data centers are secure and network-rich, ultra-reliable and energy-efficient with simply the highest standards of infrastructure design and replication. We wouldn't settle on anything less. This means your data is locked down tight, protected from even the worst natural disasters-- fire, flood, and theft.

✓ 365 Days A Year Monitoring. We believe data backups need to be monitored and checked by a qualified technician – not an automated machine. When you trust your backups and security to us, we make SURE these systems are well maintained and monitored.

✓ Fast-Restore Guarantee. We guarantee that we can get your server back up and running again within 4 hours or less. If we can't, we'll refund an entire year's service fees. Most remote backup services try to promote money-back guarantees, but if you read the small print, they only refund one month of service fees. We're willing to put our money where our mouth is and give you back a full year's service fees if we fail to make your data available.

- ✓ Our Gold Care Managed Backup plan offers free help desk support for recovering files. Some companies charge you extra for this service, or don't offer it at all.

- ✓ We will conduct monthly or quarterly test restores of your data 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.

✓ We're Local! 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 e-mail. 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 state – or different country?

A Final Word…

I hope you have found this guide helpful in shedding some light on backing up your data and making sure you could recover quickly in the event of a disaster. Clearly this is not a matter to be taken lightly, yet most business owners and organization leaders are so busy they don't think about it UNTIL a disaster happens.

As I stated in the opening of this report, my purpose in providing this information is to help you make an informed decision and avoid getting burned by the many incompetent firms offering these services.

Even if you feel everything is "okay" and that your current backup system is solid, I would encourage you to take me up on the offer of a Free Data Backup and Security Audit. This audit is, of course, provided for free with no obligations and no expectations on our part. I want to be clear that this is NOT a bait and switch offer or a trick to get you to buy something. My reputation for running an honest and trustworthy business is something I hold very dear. I would never jeopardize that in any way. So please, take a moment now to give me a call. You'll be very glad you did.

At your service,

Tim Ricketts
President, T. Daniels Consulting
810-629-0131
Email: info@tdaniels.com
www.tdaniels.com