"12 Little-Known Facts and Insider Secrets About Data Back Up and Choosing a Remote Backup Service"

If your data is important to your firm 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.
- Frightening trends 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.

From the Desk of: Mike Hughes
President, Network Titan

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 firm 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 computers. How devastating would that be?

Or, what if an earthquake or fire destroyed your office and everything in it? Or if a virus wiped out your servers…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 …)

After working with hundreds of small businesses in Southern California, we found that 6 out of 10 firms 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 firm, 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 backup system. But know this if you still happen to be using a tape backup:

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

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, tape is not the answer.

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

Frightening Trends, Cases, and Questions You Should Consider:

- 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, almost 50% of small businesses that manage their own network and use the Internet for more than e-mail will have their network accessed by a hacker, and well over 50% won't even know they were attacked. *(Source: Gartner Group)*

- About 70% of businesses have experienced (or will experience) data loss due to accidental deletion, system failure, viruses, fire or some other disaster (*Source: Carbonite*)

- 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: Ontrack Data Recovery*)

Remote Backups: What They Are And Why EVERY Firm 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), or managed backups, is a service that allows you to maintain secure copies of your data in a different location than your office.

Usually this type of backup is done automatically 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 competent 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 remote backups in the first place – is not an easy, fast, or simple job.

And to be sure, Dropbox and OneDrive are NOT back up solutions!

7 Critical Characteristics to Demand from Your Remote Backup Service

The biggest danger firms will have with remote backup services is the 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 competent, 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 sensitive information about or entrusted with your firm. Never trust your data to anyone that doesn't have the following security measures in place:

    a. Ask your service provider to what level are they compliant. At the least they should be HIPAA, Sarbanes-Oxley (SOX), Gram-Leach-Bliley (GLBA), Payment Card Industry Data Security Standard (PCI DSS and in California, the California Consumer Privacy Act (CCPA) compliant. These government regulations dictate how organizations with highly sensitive data handle, store, and transfer that data. You may be required by law to work only with vendors who meet these stringent requirements. At any rate, you will 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, and a card key system to allow only authorized personnel to enter the site.

c. Make sure the data transfer is encrypted the strongest 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 remote backup service should store multiple copies of your data in more than one location. That way, if one of *their* locations is destroyed or attacked, they have backups of your backup in a different location where the disaster did not strike.

3. **Demand the ability to receive overnight copies of your data on some type of data storage device**. If your entire network gets wiped out, you do NOT want an internet download to be your only option for recovering the data because it is very time consuming. Therefore, you should only work with a remote backup provider that will provide overnight copies of your data via some type of physical storage device.

4. **On that same note, 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 can take a long time. If you have a large amount of data to backup, it would be faster and more convenient to send it to them on a physical 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, stolen, or destroyed somehow, you're left without a backup.

6. **Demand daily status reports of your backup**. All backup services should send you a daily report to verify if your backup actually ran AND to report failures or problems. The more professional providers will also allow you to notify more than one 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 provide to confirm you are setup properly.

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 your 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 easier at night knowing you have a good, solid copy of your data available in the event of an unforeseen disaster or emergency.

Our Free Data Security Audit/Risk Assessment Will Reveal the Truth…

Want To Know For Sure about Your Data Backup?

As a prospective client, I'd like to extend a "get to know us" offer of a Free Data Security Audit/Risk Assessment. This is a way to introduce our services to you.

At no charge, I will…

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

- Check your network backups to confirm they are accurately backing up all critical files and information you cannot afford to lose.

- Discuss current data protection needs and explain in plain terms 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.

But I Don't Need a Free Security Audit/Risk Assessment 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. Some of our current clients felt they were safe until it became necessary to RESTORE their data.

Unfortunately, that is when most companies "test" their data backup and restore solution. We are helping firms like yours avoid disruptive and extremely costly data catastrophes.

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

Outstanding Customer Service No Matter The Time Or Location.

Working with Network Titan is like having your own in-house, IT department but only better. Mike and his team are focused on providing outstanding customer service no matter the time or location. Simply put, they're outstanding! Network Titan is incredibly responsive and technically sound. They consider your business to be their own. **It's hard to go wrong with Network Titan. They provide a responsive, cost-effective solution to all your IT needs.**

Jim Buechler
President & CEO at Cutwater Spirits

Network Titan Makes Us A Priority.

It is hard to pick just one benefit seeing as Network Titan is the best IT firm we could wish for. We are consistently impressed with the after-hours support, follow through on all requests, prompt responses and support. Network Titan makes us a priority. Although they have many clients, we always know they are available to us, regardless of time or day. Being a small company, IT issues can completely shut us down and working with Network Titan gives us a peace of mind. **We know we can always count on them. Don't wait for the IT catastrophe to happen, get ahead of it with Network Titan.**

Victoria Switzer
Director of Accounting
at Gomez Trial Attorneys

Our Firm Has Less Stress and Increased Productivity.

Network Titan does an awesome job! **Since engaging with this IT company we have less stress and increased productivity.** We don't have to spend the time trying to figure things out for ourselves and trying to troubleshoot. Their outstanding staff is knowledgeable, helpful, courteous, responsive and available. They have alleviated a lot of our stress over our IT issues and we feel more secure knowing they are there for us.

Hazel Martinez
Firm Operations Manager

You are Under No Obligation When You Say "Yes" to a Free Data Security Audit/Risk Assessment

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.

In order to secure a Free Data Security Audit/Risk Assessment for your firm, just contact us at 619-255-2621 or www.NetworkTitan.com/contact-us.

Dedicated to your security,

Mike Hughes
President; Network Titan
Office: 619-255-2621

P.S. Don't miss out! Your Free Data Security Audit/Risk Assessment ($500 value) will let you know for sure if your backups are working effectively and if you would be able to resume quickly after a data disaster.

Facts About Data Loss

- Over 50% of critical organization data resides on unprotected computers and laptops.
- Key causes for data loss are:
    - ✓ Hardware or system malfunction
    - ✓ Human error
    - ✓ Software corruption or program malfunction
    - ✓ Computer viruses and malware
    - ✓ Hackers and insiders
    - ✓ Natural disasters
    - ✓ Liquid damage
    - ✓ Other
- Only 25% of users frequently back up their files, yet 85% of those same users say they are very concerned about losing important digital data.
- More than 22% said backing up their computer files is on their to-do list, but they seldom do it.
- 30% of companies report that they still do not have a **disaster recovery plan** in place, and 2 out of 3 feel their data backup and disaster recovery plans have significant vulnerabilities.
- 1 in 25 laptops are stolen, broken or destroyed each year.
- Today's hard drives store 500 times the data stored on the drives of a decade ago. This increased capacity amplifies the impact of data loss, making mechanical precision and data backup more critical.
- You have a 30% chance of having a corrupted file within a one-year time frame.

Source: VaultLogix