



# “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.



**From the Desk of: Thomas Hill**  
**President / CEO**  
**CD Technology**

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 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 thousands of small and mid-size businesses in the East Tennessee area, we have 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.

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

If you are like most business owners, you've been smart enough to setup some sort of online backup service.

**However, We have found that nearly 60% of those backup methods were NOT setup properly and NOT backing up the documents needed most!**

Incredible, isn't it? Most people don't realize that ALL backup methods have some sort of failure rate. But what's really dangerous is that most companies don't *realize* that- 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.

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:**

- 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*)

## **Cloud based backups with revisions and monitoring should be used at all times.**

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 with advanced encryption technology.

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 cloud 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 cloud 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 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 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 they are HIPAA, Sarbanes-Oxley, Gram-Leach-Bliley, 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. 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.
  - 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 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 the ability to receive overnight copies of your data on DVD or some other data storage device.** 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 remote backup provider that will provide overnight copies of your data via some 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 to them on DVD.
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 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 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 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.

## **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 <Company> 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, 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 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 movies.



- 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.

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 Remote Area Medical (RAM) or ExpoQuip Inc.

## **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 this one: What I want to point out is that TennCare did not exactly have the data breach, it was caused by a company that does business with TennCare. Could this have been your company?



*The personal information of nearly 44,000 TennCare members may have compromised after a state contractor reported a security breach. According to Magellan Health Services, who the state contracts to manage pharmacy benefits for TennCare, one of its subsidiaries discovered an unauthorized access of an employee's email account who handles member information.*

*The company said it learned about the incident on July 5, 2019. The email account at Magellan Rx Management had been accessed by an anonymous third party on May 28, 2019. The company believes the employee was targeted by a phishing scam and the account was accessed to send out more spam emails.*

*The company said it was determined on Sept. 10, 2019 that TennCare data may have been compromised in the incident, and it notified the Division of TennCare a day later.*

*The email account had TennCare member information such as names, Social Security numbers, member IDs, health plan names, provider names, and drug names.*

*The company said a third-party expert found no evidence that hackers actually accessed or viewed the information in the employee's email, though.*

*The Division of TennCare said it worked with Magellan Health to get a full understanding of the incident, as well as determine which members may have been impacted to notify them.*

*"We have confidence in Magellan and this process," Sarah Tanksley with the TennCare division said.*

*Magellan Health said it is notifying those who may have been impacted by the breach and offering one year of credit monitoring services and up to a \$1 million in insurance reimbursements in the case of ID theft. Those who have questions can contact a toll-free number at 833-959-1351, which is available Monday through Friday, 9 a.m. - 9 p.m. ET*



## 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? I'm glad you asked because there are 5 BIG reasons to trust us with your data security:

1. Our state-of-the-art data center is updated and inspected regularly by a third party. This means your data is locked down tight, protected from even the worst natural disasters--fire, flood, and theft.
2. We unconditionally guarantee the security and availability of your data or your money back. If the data is given to us, we will guarantee it will be available to you 24/7 or we'll give you your money back!

Most remote backup services try to promote money-back guarantees, but if you read the small print, they only refund the last 3 months of service fees. We're willing to put our money where our mouth is and give you a full year's service fees back if we fail to make your data available.

3. We offer free help desk support for recovering files. Some companies charge you extra for this service, or don't offer it at all.
4. 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.
5. We are a local company with a real, live office. When you have a problem, we are on it in 20 minutes or less.

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?

6. 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 remote backup services do NOT offer this service.



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



Having a full time IT solutions company gave us access to an entire team of technicians to assist us, which meant that there was always someone that will be there for us when the need arises. In 2013 RAM was doing anywhere of 10 to 13 events per year and currently we have increased that to 85 to 90 events a year. With our organization continuous expansion, CD Technology was able to make sure we never fell behind when it came to our IT solution needs and security. They have been with us every step of the way.

Chris Hall - Remote Area Medical



Since working with CD Technology, we don't have to worry about the IT part of our business. We can focus on our main goal and that is residential property management. We had always handled managed IT internally, but that took our focus away from our main business. I would absolutely recommend CD Technology. They are always quick to respond and take care of all our IT needs with professionalism and thoroughness.

Benita Moody - Apex Property Management



CD Technology staff is knowledgeable, friendly, and experienced, always there to help. You can rely on this team for all your IT needs. They keep in touch every step of the way and are available anytime you have a computer issue that needs to be resolved. We recently had a serious problem with our network server. **They worked all weekend to get the issue resolved so we didn't have any downtime, and we were up and running on Monday like nothing had happened!**

David Buckner, David Buckner CPA



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

We also 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.

**Call our team immediately at (865) 909-7606  
and schedule your free, no obligation service.  
At least then you will know where you stand.**

Sincerely,

Thomas Hill  
Thill@CDTechnology.com

P.S. Don't miss out!!! Your Free Data Security Analysis (\$500 value) will let you know for sure if your backup really is copying and storing all of the data you cannot afford to lose in a format that can be restored.

## Scary But True Facts About Data Loss

- The average failure rate of disk and tape drives is 100% - ALL DRIVES WILL EVENTUALLY FAIL.
- Only 34% of companies test their tape backups and, of those who do, 77% have found failures.
- 60% of companies that lose their data will go out of business within 6 months of the disaster.
- Over ½ of critical corporate data resides on unprotected PC desktops and laptops.
- Key causes for data loss are:
  - 78% Hardware or system malfunction
  - 11% Human error
  - 7% Software corruption or program malfunction
  - 2% Computer viruses
  - 1% Natural disasters
  - 1% 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 PCs was on their to-do list, but they seldom do it.
- 30% of companies report that they still do not have a disaster recovery program in place, and 2 out of 3 feel their data backup and disaster recovery plans have significant vulnerabilities.
- 1 in 25 notebooks 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 more critical.
- You have a 30% chance of having a corrupted file within a one-year time frame.

Source: VaultLogix



**“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.

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 movies.
- 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.

Call 865-909-7606 Today