COMPUTER DEPOT INC.
Locations in Knox and Sevier County

"12 Little-Known Facts and Insider Secrets *Every* Business Owner Should Know About Backing Up Their Data and Choosing a Cloud 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 backup services and cloud storage services 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.

June 2021

Thomas Hill Jr.
President/Project Manager
Computer Depot Business Solutions

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 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 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 businesses in the Knox and Sevier county 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 $3000 and $15,000 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.

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 Cloud Backup Service

The biggest danger businesses have with cloud 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 cloud 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 Cloud 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 Network Security Assessment Will Reveal the Truth…

As a prospective new client, I'd like to extend a "get to know us" offer of a Free Network Security Assessment. I am not normally in the business of giving away free services at Computer Depot Business because if I did, I'd go out of business. But this is the one way I can show you the value and security our company can offer you with no risk to you.

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

- Audit your current Network Security procedures that you may or may not have in place.
- Review your backup procedures that are already in place.
- Examine Desktop and Server computers for missing patches and security vulnerabilities.
- Evaluate your email service to determine if it is setup properly and protected from Spoof attacks.
- Plus, so much more.

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.

But I Don't Need a Free Network 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. 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 Cloud Backups To Us?

There are a lot of companies offering cloud 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. 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!

   We will refund up to 12 months of your Data Backup Fees as outlined in our service agreement.

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 team to get all your data restored in the unfortunate event of a catastrophic loss.

4. We are a local company with a real, live office located in the Knox and Sevier county area. 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 or phone.

   We'll come on site, give you a FREE network assessment and help you determine the best course of action to secure your company and customers data. 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?

5. 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…

BEYOND NO WORRIES
For our practice, having Computer Depot means NOT having to worry about HIPAA compliance, IT issues, or software updates. What really sets them apart though, is how quick and thorough they solve problems. Calls or emails are answered promptly, and concerns are addressed in an easy to understand manner. The customer service at Computer Depot can not be beat!

Dr. Krystal Barton OD

PEACE OF MIND
When most practices in our industry think about computers, IT issues, and HIPAA compliance, they probably don't have thoughts of happiness and peace of mind. For us, knowing that Computer Depot is there to answer questions and help with updates and security has been paramount. We truly have peace of mind! We have been so happy ever since they started helping us. Computer Depot is the way to go in terms of service, friendliness, responsiveness, and professionalism.

Brittney Fleetwood Admin Manager
The Nursing Center at Little Creek

TECHNOLOGY "GO- TO"
Exceptional customer service! Thomas and the entire team at Computer Depot are THE Information Technology "Go-To" in East TN. They consistently provide professional, prompt, and accurate solutions to any technological question or concern we may have. We rely on Computer Depot for all of our IT needs!

Jackie Page Practice Manager
The Lucas Center Plastic Surgery

You are Under No Obligation to Do or Buy Anything When You Say "Yes" to a FREE Network Assessment

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

Thomas Hill Jr.
Computer Depot Business Solutions
thill@computerdepotonline.com
865-512-6522 press 6