PROTECT YOUR DATA

"12 Little-Known Facts *Every* Business Owner Must Know About Data Backup, Security & Disaster Recovery"

Discover What Most IT Consultants Don't Know Or Won't Tell You About Backing Up Your Data And Recovering It After A Disaster

A Letter From The Author:

Why Did We Create This Report And Who Should Read It

From The Desk of: Michelle Sherman
President,
Computer Services Unlimited, 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 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. And even though many people KNOW they should be backing up their data, we have found that most business owners are grossly misinformed about data back and (more importantly) disaster recovery.

That's why we created this report. We wanted to give CEOs and executives an informative, easy to read guide that would explain what they need to know about backups, security and business continuity (a $.50 word for keeping your business up and running).

Just by asking for this report you are putting yourself far ahead of most business owners who never get around to thinking about this issue until it's too late. For that, I congratulate you and hope that you find in this report the information and the encouragement that you need to put the proper systems in place now so you can sleep easier at night knowing you're prepared for the worst.

Dedicated to serving you,

Michelle Sherman

But That Could Never Happen To Me!

(And Other Lies Business Owners Like To Believe About Their Businesses…)

After working with over 300 small and mid-size businesses in Fairfax County and the surrounding area, we have found that 90% of business owners we talk to do NOT have a reliable backup of their data and do NOT know how or what they would do in the event of a data-erasing disaster. They simply "think" their backup is/was working and that it will save their bacon when disaster strikes. **This "I think so" approach is incredible when you consider how dependent businesses are on information** – be it client databases, accounting records, e-mails, pictures, inventory, blueprints, and other work products – almost ALL processes in a business rely on the availability of digital information.

The cost of losing that information (or being without it for an extended period of time) is hard to accurately quantify since it affects so many aspects of a business. But we do know this: 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). Here are some other statistics about losing data:

Did You Know That…

- Tape drives fail at an average rate of 100%; that means ALL tape drives fail at some point and do NOT offer complete protection for your data if a natural disaster, water damage or fire destroys your office and everything in it.

- 20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years*. (Source: Richmond House Group)*

- 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 half 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*)

- The first reaction of employees who lose data is to try to recover it themselves by using recovery software or restarting or unplugging their computer — steps that can make later data recovery impossible. (*Source: Survey by Minneapolis-based Ontrack Data Recovery*)

"But I Already Back Up My Data," You Say…

If you're smart, you have some type of backup system in place. That's good. HOWEVER, there's a HUGE difference in the quality and reliability of backup systems and services. Plus, data backup is only ONE aspect of what's REALLY important: disaster recovery, or your ability to RESTORE the data in a usable format quickly and painlessly.

In this report I'm going to give you a number of things you need to know about choosing a good backup solution, as well as what you need to know in order to choose the right company to set up and

manage your backup.

Why You Need To Get Rid Of Your Tape Backup

One of the most common forms of backup is tape drive backups**. Yet most business owners don't know that the average failure rate for a tape backup is 100% – ALL tape backups fail at some point in time**. Incredible, isn't it? Most people spend their days dutifully swapping out tapes and taking them home day in and day out only to discover their data wasn't being backed up. But what's really dangerous is that most companies don't *realize* their tapes have failed 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 a tape or external hard drive backup system in place, but were sickened to find out it wasn't working when they needed it most.

Here are the top reasons why tape backups are a BAD idea:

- Tape drives are extremely unreliable for data backup. It's *very* common for a tape drive to malfunction without giving any warning signs whatsoever. In fact, many tapes will *contain* data, but won't allow you to *retrieve* that data.

- If your office (and everything in it) gets destroyed by a fire, flood, hurricane, tornado, or other natural disaster, your tapes or other external backup devices that are stored onsite will be destroyed as well.

- Tapes are highly susceptible to heat, moisture and dust; since most people transport tapes offsite in a purse or car, these elements destroy the tapes and the data on them.

  Side Note: Storing tapes in a fire-proof safe or filing cabinet will NOT keep them safe. These storage devices are designed to protect PAPER which has a very high heat tolerance and won't catch fire unless directly in contact with a flame. The heat from the fire will destroy the tapes and melt the plastic, which causes a double disaster since the tapes melt all over the papers in the safe.

- Human error: Someone in your office accidentally formats the tape, erasing everything on it, forgets to swap them out, forgets to take them home, goes on vacation or leaves permanently.

- Tapes are NOT secure. If any data is leaving your office, it needs to be secure and encrypted. This goes double if you're storing client information. Clients are very sensitive to their personal information being stolen, even if it's only e-mail addresses and purchase history. And if you're storing financial information, credit card numbers, medical records or other highly sensitive information, you're actually breaking the law by using unsecured tape to copy and transport this data offsite.

Backing Up To The "Cloud:" What It Means And Why EVERY Business Should Have It In Place

One of the BEST ways to protect your data is to maintain an up-to-date copy in a high-security data center somewhere other than your office. In fact, it should be in another "safe" city at least 180 miles away from your office, and ideally one that is not susceptible to natural disasters like hurricanes, floods, tornados or earthquakes. The generic term people use to describe this type of backup is "backing up to the cloud" or "cloud backups," which simply means that your data is hosted in a remote data center and accessed via the Internet.

This type of backup is set to run automatically either after hours, when most people are not using their computer systems (1:00 a.m. for example), or continuously throughout the day whenever a file is changed or added. The data on a particular machine is copied and sent over the Internet to a high-security facility where it is stored. Because these backups are automated, you don't have to worry about someone forgetting to run the backup.

As with anything, you get what you pay for, and there are some key quality differences in the type of backup service you choose. Pick the wrong one and 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.

12 Critical Characteristics To Demand From Your Backup Service And IT Company

So what should you look for when choosing a company or service to backup and secure your data offsite? Who can you trust to not only keep your data safe, but also to be there when you need to recover it?

Unfortunately, this is not an easy choice. There are literally hundreds of companies offering backup devices, software and services because they see it as an easy way to make a quick buck. As you would expect, not all service providers are created equal, and you want to make sure you choose a good, reliable vendor or you'll get burned by hidden fees, unexpected "gotchas," difficult and slow recovery of your data or by the horrible discovery that your data wasn't even being backed up properly, leaving you high and dry when you need it most. Here are 11 things we recommend looking for:

1. **Production-Grade, SAS 70 Data Center.** One of the first things you need to ask your IT person is, "Where will my data be stored?" After all, we are talking about your financial information, client data, and other sensitive information about your company! What you DON'T want is for them to keep your data at a rack in their office that is not designed to be a high-availability data center. A TRUE data center will be 100% dedicated to hosting data and should have:

    - ✓ Redundant power sources and generators
    - ✓ High-level, on-site building security
    - ✓ Redundant Internet access
    - ✓ SSAE 16 Type 2 certification

    The term "SSAE 16" (Statement on Auditing Standard) refers to an official document issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). The AICPA sets out the auditing standards for data centers and issues this document to show that the data center is doing what they are promising in the areas of security and availability.

2. **Bare metal imaging.** This is important to ensure a quick restoration of your data and IT operations. A "bare metal" image is simply a snapshot of your server and all the data on it. That snapshot can then be copied to another server or "virtualized" (put on a server online), often within 1 hour. Without this type of backup, you would have to:

    - ✓ Locate all your software disks and keys
    - ✓ Re-install the operating system
    - ✓ Re-install all applications
    - ✓ Re-install the data
    - ✓ Re-configure the settings

    This process could take anywhere from one to two days; even longer if you don't actually HAVE your software discs and keys. A bare metal image eliminates this delay.

3. **The ability to recover data FAST**. An EXTREMELY important question to ask is, "If my server crashes beyond repair, how do we get our data back?" You do NOT want Internet download to be your only option for recovering data from the cloud because it could take days or weeks. At a minimum you should be able to get an overnight copy of your data on a physical disk or device – but ideally you should have instant access to a bare metal image so that a new or makeshift server can be set up within an hour, allowing you to keep working (see above).

4. **Continuous backup.** Another feature to look for is ongoing or "continuous" backup versus a nightly backup. This allows you to restore a file that you worked all morning on and saved right before the server crashed in the late afternoon.

5. **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, city-wide power outage or natural disaster destroys one of *their* locations, they have backups of your backup in a different city where the disaster did not strike.

6. **The INITIAL backup should be to a local, physical device**. Trying to transfer all the data online could take days (possible weeks) and cause your Internet connection and systems to drag. If you have a large amount of data to backup, ask your provider how the initial backup is created.

7. **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 damaged in a fire, stolen, or destroyed in a flood, you're left without a backup.

8. **The ability to "virtualize" your server**. This is a fancy term for putting your server online so that you and your staff can work remotely if necessary. This option would be important if your building was destroyed or if your area was evacuated.

9. **Demand a local "spare" server and backup.** Most server crashes are due to hardware failure, not natural disasters. Therefore, you should have an onsite, local backup server as a failover device if your main server dies. This local server also makes it much easier to retrieve a file or folder than trying to pull it down from the Internet (see #3).

10. **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.

11. **Demand LIVE monitoring by a qualified technician**. Many online backup services are "self-serve," which allows them to provide a cheaper service to you. BUT backups are not "set it and forget it" processes so don't settle for an "automated" monitoring service. All too often problems happen with backups that require someone who knows what they're doing to investigate the problem and resolve it. Otherwise, you simply have an alarm system that no one responds to.

    Plus, if you need to recover your data, you want to be able to call and talk to someone who can help you, especially if it's a major disaster. If you're using a cheap online backup service or a company that doesn't offer live monitoring, you'll be stuck trying to recover your data on your own, wasting tons of time and possibly not being able to get back up and running for days.

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 recoverable. 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 weekly restores should be done. If your situation is a little less critical, then monthly or quarterly test restores are sufficient. Any number of things can cause your backup to become corrupt. By running a test restore, 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 Audit 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 Security Audit ($275 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 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.)

- 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 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.

- 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 ABRA (Advanced Backup Recovery Appliance) Solution.

Naturally, I don't expect everyone to become a client; you won't be pressured into buying anything or driven nuts by a pushy, desperate sales guy. Of course we'd love to have you as a client, but our primary goals are to provide value in advance, to educate you and other business owners and to provide smart, affordable options for making sure your business doesn't lose critical data.

How To Request Your Data Backup And Security Audit

To request this, simply do one of the following:

1. Call our office at 703-968-2600.

2. Send us an e-mail to helpdesk@csuinc.com

3. Go online to www.csuinc.com and fill out the form on our homepage.

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:

- ✓ **High-Availability, High Security Data Center.** We have three cloud data centers that we upload your data too; one in Atlanta, GA, one in Salt Lake City, UT, and the other in Kansas City, KA. These facilities are designed for 99.999% reliability. This means your data is locked down tight, protected from even the worst 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 2 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.

- ✓ **Free Help Desk For File Restores.** Need help in restoring a file you accidentally deleted or over wrote? Call our help desk and we'll restore it back to you. Some companies charge you extra for this service, or don't offer it at all.

- ✓ **Regular Test Restores And Daily Reporting.** We insist that all clients receive weekly or monthly (your choice) test restores of their backups to ensure they are working. We also send all of our clients a daily e-mail that verifies that their backups ran without errors. Of course if they don't, we're on it immediately.

- ✓ **We're Local!** We often joke that clients like to have a vendor within "choking distance." Not only are we local with an office in Chantilly that you can visit, but we've also been serving small and medium businesses in this area for over 20 years. 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 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.

Dedicated to serving you,

Michelle Sherman
Computer Services Unlimited, Inc.
703-968-2600
www.csuinc.com