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, costliest mistakes that most small business owners make with their data backups.

Read this guide and you'll learn:

- What remote, off-site, or managed backups are, and why *EVERY* business should have them in place.

- **Seven 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 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.

Curtis McCallister, MCSE, CCA | Manager of Technology Solutions
James Moore & Co., P.L.

From the Desk of: Curtis McCallister, MCSE, CCA
Manager of Technology Solutions, James Moore & Co., P.L.

Dear Colleague,

Have you ever lost an hour of work on your computer?

Now imagine if you lost days or weeks of work – or 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 *when*.

After working with over 200 small and mid-size businesses throughout North Central Florida, 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 **$9,000 and $60,000** in repairs and restoration costs on average.

That doesn't even include lost productivity, sales, and client good will 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 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 ALL drives fail. But what's really dangerous is that most companies don't realize it has happened 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 they were sickened to find out it wasn't working when needed the most.

Technology Solutions Consulting Team
🌐 www.jmco.com
✉ info@jmco.com

📞 Daytona Beach 386.257.4100
📞 Gainesville   352.378.1331
📞 Tallahassee   850.386.6184

James Moore
Technology Solutions

While you should maintain a local backup of your data, a backup will NOT offer you protection if...

1. Your drive malfunctions, rendering it useless and making it impossible to restore your data. IMPORTANT: It is very common for a drive to malfunction without giving any warning signs.

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

3. The physical drive you are backing your data up to becomes corrupt due to heat or mishandling.

4. The backup job never completes because the drive is too slow to finish the job.

5. Someone in your office forgets to change the drive and it gets overwritten, or the drive is never inserted so the backup doesn't even run, or he/she inserts the wrong drive...

6. 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 that your backup was not working when you need it most.

Technology Solutions Consulting Team

www.jmco.com

info@jmco.com

Daytona Beach 386.257.4100

Gainesville   352.378.1331

Tallahassee   850.386.6184

James Moore
Technology Solutions

3

- **Drives fail on average at 100%**; that means ALL drives fail at some point and do NOT offer complete protection for your data if a natural disaster, fire, or random accidents destroy your office and everything in it. Business owners who were hit by hurricanes like Katrina learned a hard lesson about keeping remote backups of their data.

- **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-size 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 by restarting or unplugging their computer — **steps that can make later data recovery impossible**. (Source: 2005 global survey by Minneapolis-based Ontrack Data Recovery)

Technology Solutions Consulting Team
www.jmco.com
info@jmco.com

Daytona Beach 386.257.4100
Gainesville 352.378.1331
Tallahassee 850.386.6184

James Moore
Technology Solutions

4

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 off site in a high-security facility.

Remote backup, also called off-site backup, online backup, or managed 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 done automatically after hours via the Internet to a high-security facility. There is no question that every business owner should have an off-site copy of their data; however, there ARE big differences among remote backup services. 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 remote backups in the first place – is not an easy, fast, or simple job.

SEVEN 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 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 seven of these points, then you'd be crazy to trust them to store your data:

Technology Solutions Consulting Team
🌐 www.jmco.com
✉ info@jmco.com

📞 Daytona Beach 386.257.4100
📞 Gainesville 352.378.1331
📞 Tallahassee 850.386.6184

James Moore
Technology Solutions

5

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:

   - 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 your organization does NOT fall under one of these categories, you still want to choose a provider who meets these regulations, because it's a good sign that they have high-level security measures in place.

   - 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.

   - 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. This means 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 to recover 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 back up, 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 from which it was backed up**. Amazingly, some backups can only be restored to the same computer from which they came. If the original computer was burned in a fire, stolen, or destroyed in a flood, you're left without a backup.

Technology Solutions Consulting Team
🌐 www.jmco.com
✉ info@jmco.com

📞 Daytona Beach 386.257.4100
📞 Gainesville   352.378.1331
📞 Tallahassee   850.386.6184

James Moore
Technology Solutions

6

6. **Demand daily status reports of your backup.** All backup services should send you a daily e-mail to verify that your backup actually ran AND to report failures or problems. More professional providers should also allow you to notify more than one person (like a technician or your IT person) in addition to you.

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 can 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…

Technology Solutions Consulting Team

www.jmco.com

info@jmco.com

Daytona Beach 386.257.4100

Gainesville 352.378.1331

Tallahassee 850.386.6184

James Moore
Technology Solutions

7

Because you are a prospective client, I'd like to extend to you a "get to know us" offer of a Free Data Security Audit. I thought this would be a great way to introduce our services to you.

At no charge, a security specialist will visit you 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 that you would NEVER want to lose.

- Present a simple and easy to understand chart detailing the makeup of your data, including the ages and types 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 of 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 discuss areas 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 managed Backup and Disaster Recovery (BUDR) service.

Technology Solutions Consulting Team
www.jmco.com
info@jmco.com

Daytona Beach 386.257.4100
Gainesville 352.378.1331
Tallahassee 850.386.6184

James Moore
Technology Solutions

8

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 these:

True Story: In January of 2016, James Moore restored three years of scanned back up files for The City of Flagler Beach. I discovered that a data file to my financial software, BS&A, was gone and from the looks of things had disappeared sometime around December 15, 2015. The file contained over three years of scanned attachments for the Purchase Order Module, which was an extremely important file. When I contacted the current IT consultants, they told me that if the file disappeared prior to December 25th (which it did) then it was gone for good. In desperation I reached out to Jerry Pflueger, our IT consultant for many years with James Moore, to see if there was anything he could help with a possible solution. Luckily, James Moore was able to direct the new consultants to the backup hardware that contained the file in question. James Moore also assisted the consultants in restoring the backup and extracting the data file. Although they did not have to step in and help, I am truly thankful to James Moore for the restoration of three years of scanned backup and the impeccable customer service they provided.

True Story: James Moore began managing a new client whose network was built by another company. The main business software was installed on the same server that held the company's email and business files. One of our first steps when bringing on a new client is to set up our managed Backup and Disaster Recovery (BUDR) service, which was a good thing because a few short weeks after we started supporting them, their primary business application was being updated and crashed. When the business application update crashed, it took the Windows server with it, causing the client to lose access to not only their business application but their email and of business files. James Moore restored that server into a virtual machine and had the client back up in a few short hours. We then rebuilt the server and added a new server just for the business application so this would never happen again.

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!

Six BIG reasons to trust us with your data security:

1. **We have the experience you can count on.** Having been in business for half a century working with sensitive personal and business information, we know how important it is to keep that information not only private but safe from loss or damage. A recent Gallup study shows, again, that most new businesses fail in the first years; we've been in business ten times that and we're still going strong.

2. **We understand the importance of maintaining business continuity.** We not only protect your business information, we help you put strategies in place that can keep your business running even if a disaster closes the doors to your local office.

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.** That might not seem too unique to you, but what you don't realize is that some off-site 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 visit you 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.

James Moore
Technology Solutions

BUT DON'T JUST TAKE OUR WORD FOR IT - LOOK WHAT OUR CLIENTS HAVE TO SAY...

"We have been using the accounting and auditing services of James Moore for many years. When we decided to outsource our IT needs, it was a surprise to me that James Moore had entered the world of technology solutions. Since James Moore had served us so well in the past, I was sure they could do the same in this area too. We have not been disappointed. Their staff is very knowledgeable, easy to work with and quick to respond to our needs."

Lori Emmer McGriff, President, Emmer Development Corp.

"[James Moore & Co. Technology Solutions Consulting Team] has been a true technology partner for CPPI for many years. Throughout our partnership [they] have been an integral part in assisting with many IT projects and initiatives. JMCO-IT helped with office relocations, advanced network support, complex troubleshooting projects, and [they're] always extremely responsive, professional and friendly. JMCO-IT is highly skilled and friendly; I would recommend them without hesitation."

Brad Buckles, Director of Technology, Charles Perry Partners, Inc.

"...For the last 10 years we have been hosting our email on our own servers using Microsoft Exchange. We recently decided to make the switch to Office 365 Business Premium based on the recommendation of James Moore and Co. The transition was nearly transparent to my users...and trouble-free...[their team was] fast and always available to quickly answer questions...there literally were zero problems...I never spent a single night waiting on an email reply or worrying about an issue."

Jerry Everetts, COFB, IT Director, Food Supply, Inc.

Technology Solutions Consulting Team
www.jmco.com
info@jmco.com

Daytona Beach 386.257.4100
Gainesville 352.378.1331
Tallahassee 850.386.6184

James Moore
Technology Solutions

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 backups and, of those who do, 77% have found failures.

- 60% of companies that lose their data will go out of business within six months of the disaster.

- More than half 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 two out of three feel their data backup and disaster recovery plans have significant vulnerabilities.

- One 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

YOU ARE UNDER NO OBLIGATION

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.

However, I cannot extend this offer forever, because time and staff limitations simply won't allow it. In order to secure your Free Data Security Analysis for your company, you must respond to this letter by June 30th. Spots ARE limited so act today. I regretfully will have to withdraw this offer and make it available for someone else if you are unable to respond on time.

Call me the Help Desk immediately at 800-455-5676 to schedule your free service, or go online and complete the form to secure your place: **www.tinyurl.com/huwc945**

Sincerely,

Curtis McCallister, MCSE, CCA
Manager of Technology Solutions
James Moore & Co.
Direct: 352-378-1331 x2255

Sign up now and you'll be glad you did:

http://tinyurl.com/huwc945