"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.

David Steger
Founder and President,
ManagePoint

Dear Fellow Business Owner

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 over 200 small and mid-size businesses in the Milwaukee, SE Wisconsin and Chicagoland areas, 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 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 set up a tape backup. But know this:

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 don't realize that ALL tape drives fail. But what's really dangerous is that most companies don't *realize* it 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 were sickened to find out it wasn't working when they needed it most.

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

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

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

3. The physical tapes you are backing your data up to become corrupted due to heat or mishandling.

4. A virus spoils the data stored on the tape drive. Some of the more aggressive viruses not only corrupt the data, but they don't allow anyone to

access the data on the drive.

5. Someone in your office accidentally formats the tape, erasing everything on it.

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

Frightening Trends, Cases, and Questions You Should Consider:

- Tape drives fail on average at 100%; that means ALL tape drives fail at some point and do NOT offer complete protection for your data if a natural disaster, fire, or terrorist attack destroys 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 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: 2010 global survey by Minneapolis-based Ontrack Data Recovery*)

Remote Backups: What They Are And Why EVERY Business 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, or managed backups, 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 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 remote 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 remote 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 ManagePoint 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 with our *BackupPoint* service.

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 Engman-Taylor Co. or Quest Industrial Products.

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 these:

> "We were doing a routine Windows update on our server and could not get the server restarted. Key files in the operating system had been corrupted during the upgrade. The ManagePoint team was very responsive and worked over the weekend and got it working again. We're very pleased with both their tenacity and the teamwork and we now are working with ManagePoint to build more robust backups, which we previously lacked." - **Rich Sweeting, President, Millennium Die Group**

Here is yet another…

"I thought our network was absolutely secure UNTIL one of our employees accidentally downloaded a nasty worm. Within seconds, our entire network was compromised; but thanks to ManagePoint , were able to quickly recover and avoid a lot of embarrassment, costs and downtime. Now we have the proper security systems in place and are being monitored and I sleep a lot easier at night! **Angie Van Scyoc, *CEO, Geriatric Support/ Pathway Care***

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…<Outline how/why your data center is secured. It doesn't have to be unique to you, but it does have to impress them>. 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. <You may need to revise this if you are not local, or swap it out with other guarantees or a USP>. 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, 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…

"In financial services, you need someone who can respond quickly."

"When our company first started up we were working with another IT company, but everything started to fall apart. Our clients were coming in and our network was not set up, but ManagePoint came in and had us up and running in short order. When you are dealing in financial services and with personal data, you need someone who can respond quickly and help you with backups. You can't have downtime in our industry. Payroll happens every day and people depend on it, so when something goes down, we need immediate response. That's what ManagePoint gives us. We recently accidentally deleted a critical file, but they were able to pull it off of our backup and within 30 minutes we were up and running again! They took care of us right away."- **Pete Feaman, CPA, Vice President, Integrated Payroll Services**

"ManagePoint has our backs covered!"

"Our first project with ManagePoint was getting a new firewall and mail filter in. We were quite pleased with how everything went. They showed real expertise, got us migrated over flawlessly and it has been running rock-solid ever since. Then they upgraded our backup system. Our old Quantum tape backup system had died and what they replaced it with has been running perfectly. More recently, ManagePoint updated our switching fabric with a leading-edge 3-server setup on 10gig Ethernet. It's awesome! It runs rock-solid. I love the thing! Our switch logs almost zero errors. Our video editors no longer complain about stuttering. Our production department is very happy. I'm glad I decided to talk to ManagePoint! They came up with a cheaper and better solution than what Apple had proposed. I couldn't be happier with that decision. I feel that ManagePoint has our backs covered. If we have an emergency, their response time is awesome. It's a good feeling to have ManagePoint as a safety net." ----**Mark Sternig, IT Manager at The Sportsman Channel**

"ManagePoint knows what they are doing!"

"ManagePoint provides for us SecurPoint, a managed security solution, to handle all our routers, firewalls, switches and wireless access points. We do not have the expertise, which would require us to get a tremendous amount of education. We do not want to be experts in that. We maintain a small IT staff to focus on strategic applications specific to ETCO. We do not want to learn every platform, operating system, and hardware device that we have in our environment. ***We just want it to work!*** We knew we needed somebody to watch over the security of our network and make changes and let us know when there are issues. We trust ManagePoint knows what they are doing and that has proved to be the right decision."
Julie Guenterberg, IT Systems Manager, Engman-Taylor Company

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.

However, I cannot extend this offer forever because time and staff limitations simply won't allow it. 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 immediately at (414) 456-9837 to schedule your free service, or complete and fax back the enclosed form.

Sincerely,

David Steger

David Steger
Founder, President
david.steger@manage-point.com
Direct Line: (414) 456-9837