PROTECT YOUR DATA

"12 Little-Known Facts Every Business Owner Must Know About Data Backup, Security And 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

"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.
- 6 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.

From the Desk of: Gary Gomes
Owner
Flag Computer Repair

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 over 90 small businesses in the Ashford, Kent 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 in repairs and restoration costs.

That doesn't even include lost productivity, sales, and client goodwill that can be damaged when a company can't operate or fulfil 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 to an external drive. But know this:

ALL hard drives fail at some point in time.

Incredible, isn't it? Most people don't realise that ALL hard drives fail. But what's really dangerous is that most companies didn't *realise* it happened until it's too late.

That's why history is riddled with stories of companies losing millions of pounds 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, an external drive 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 hard drive to malfunction without giving any warning signs.

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

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

4. A virus spoils the data stored on the hard 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 drive, 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:

- ALL hard drives fail at some point and do NOT offer complete protection for your data if it is stolen, or a natural disaster or fire destroys your office and everything in it. Business owners who were hit by theft 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: 2005 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, cloud 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.

Microsoft OneDrive, Google Drive, Dropbox, etc are **NOT** backup services. They only synchronise your data between the computer and the cloud. If you delete a file on the computer, it immediately deletes the same file in the cloud.

Microsoft only keeps that deleted file for 30 days or 93 days depending on the type of account you use, and settings enabled!

6 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 6 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 GDPR compliant. These are government regulations that dictate how organisations handle, store, and transfer their data.

b. Make sure the physical location where the data is stored is secure.

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 centres 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. **Ask your service provider if you have the option of having your *initial* backup performed through hard copy**. 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 a hard drive.

4. **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.

5. **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.

6. **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 Cyber 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 Cyber Security Assessment. I don't normally give away free services at Flag computer Repair because if I did, I'd go out of business. But 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, and maintenance schedule to see if there is anything jeopardising your data's security.

- Review procedures for storage and transportation of data. Many people don't realise 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.

- 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 secure backup 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 a loyal client.

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:

> The owner of an Aldington based company thought their 5-year-old SSD was working safe and sound. Remember ALL hard drives fail. Without warning a failure of the drive occurred. However, no need to panic as they were using my secure backup service. A new drive was purchased, and a clone made from the previous days image. The computer was up and running within 2 hours. What would happen if your drives failed without warning?

Here is yet another…

> Another client of ours learned about the benefits of a secure backup service. An all too common occurrence are Windows updates going wrong and corrupting the operating system beyond repair. The only alternative is to wipe and reload but what about all that data that’s lost with it? Fortunately maintaining a backup, as this client found out, saves the day. With a reload and backup restoration, they were operating again.

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 4 BIG reasons to trust us with your data security:

1. We partner with Acronis, an internationally renowned data protection service. You may know that they also provide data protection for the Williams F1 team. With multiple data centres in multiple geographic locations, guarded 24/7, providing redundancy. We also partner with Skykick for unlimited backup and retention of Microsoft 365 accounts. This means your data is locked down tight, protected from even the worst natural disasters--fire, flood, and theft.

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 are a local company and offer onsite visits. We'll come on site and shake your hand. 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 County – or different country?

4. 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…

Responsive, Expertise, High Level of Service

I am very pleased and comforted to have engaged the services of Flag Computer Repair as on the occasions that I have asked Gary to sort out a problem with my computer he has been very responsive and efficient in dealing with it. His patience, expertise and very pleasant manner has always been appreciated. I have not experienced with any other IT company the satisfaction and high level of service that I have received from Flag Computer Repair. **I would have no hesitation in recommending Flag Computer Repair** to anyone and suggest they contact Gary immediately to discuss your needs. I am totally confident that you will be happy with the knowledge and business arrangement that he could offer.

Ian, Willesborough Lees

Informative, Knowledgeable, Proactive

The single biggest benefit to me since using Flag Computer Repair is to have a friendly, local, independent IT person on hand at a moment's notice. I feel Flag Computer Repair is better than other IT firms I have worked with in the past, at being informative, knowledgeable and proactive. If you are on the fence about choosing them as your IT firm, I would say, Gary is a friendly, approachable person, he is very helpful, will deal with the task in hand and will make suggestions where necessary. **Highly recommended**.

Sarah, Kingsnorth

Professional, Reliable Service, Expertise.

Flag Computer Repair offers a very professional and reliable service with extensive knowledge and broad experience of the IT world. The service is tailored to your individual requirements and without exception, Flag Computer Repair has been able to solve every problem and answer every question in an efficient and easily understandable way.

Other IT computer firms may have been able to solve problems but in virtually every case I've come across, they talk in a language that's almost impossible for the layperson to understand. **Flag Computer Repair is excellent at explaining what the issue is and offers easy to understand solutions.** Nothing is too small or large for them to solve: the best service I've ever had. It's a pleasure using Flag Computer Repair for my IT rather than the chore it can be with other IT companies who can often get frustrated with the client for not understanding their language. Other companies have been quite condescending and poor at communicating in the past when I haven't understood what they're explaining (badly). I don't expect them to understand my business, but they expect me to understand their IT gobbledygook.

If you are on the fence about choosing Flag Computer Repair, I would say do not hesitate. If you want a service that offers wide ranging expertise, efficiency and good value for your money and speaks in a language you will understand, then get off that fence!

Shirley, Aldington

You are Under No Obligation to Do or Buy Anything When You Say "Yes" to a Free Cyber Security 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 or email me immediately at **07976 151148** to schedule your free assessment.

Scary But True Facts About Data Loss

- The average failure rate of disk 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 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