

Business Advisory Guide

“9 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

Author: Jan Chapman
Technical Director
MSP Blueshift
1300 501 677
www.mspblueshift.com.au

A Letter from the Author:

Why Did We Create This Report and Who Should Read It

Dear Colleague,

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

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 server. How far would that set your business back??

Multiply the hourly cost of your staff not able to work and worst still having to rework entering data all over again.

Or, what if a major storm, flood, or bushfire 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 have confidence in?

How quickly do you think you could recover if you can't recover at all?

If this is the first time you are considering these questions or you don't have 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 backup and (more importantly) disaster recovery.

That's why I created this report. We wanted to give CEOs, business owners and executives an informative, easy to read guide that would explain what they need to know about backups, security and business continuity (i.e. keeping your business up and running).

By reading 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. But more importantly once you have read this report, if you believe you need to take action, don't delay.

We have seen first-hand what can happen when a business is at risk; when the words 'It will never happen to me' are replaying through your head as you are working 24/7 trying to keep your business running.

I hope that you find the information in this report useful and encourage you to consider the 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,



Jan Chapman

About the Author

Jan Chapman is one of the most highly qualified and experienced IT professionals in Australia, today. He started his IT career in 1997, but before that spent 13 years in the British army, working on the electronic and optical sighting systems for fighting vehicles, such as main battle tanks. This included taking part in the first gulf war and spending six months in Bosnia with the UN. These were challenging places to work with extremes in temperature; very rough living conditions, in a war zone. These conditions tested his abilities to the full.

In 1997 Jan left the army and took up a new career in Computers, the transition was seamless as he had already had many years of experience with computers at the electronic component level. Initially he worked in Oxfordshire with a small outsourcing company, the work then was mostly installing Novel servers, upgrades to windows 95, connecting businesses to the Internet and setting them up with email, as they transitioned away from letters and paper memos.

Jan moved to Australia in 1999 and immediately started working for MITS (later to be bought by Logica) another outsourcer but much larger. This is where his expertise with the corporate sector was honed. Providing IT support to businesses such as City West Water, Vline Passenger and Yarra Valley Water. Then moving into consulting and project management with other Logica clients such as Holden Motors, TXU and the Department of Justice.

After 5 years with Logica Jan moved to a smaller IT outsourcing company to manage the technical team. This is where he developed his leadership and team building skills, getting the right people and developing a high performing team. This also required him to develop systems and quality procedures the underpinning foundations for good teamwork.

In 2009 Jan co-founded MSP Blueshift, with the aim of providing a quality managed service to small businesses at a reasonable price, with the mission of delivering a level of service that all of their clients would recommend to others. The many years of past experience have helped build the success his business is currently experiencing. Formal systems and processes (for everything) are critical, together with the right people doing the right jobs, and using computers to automate tasks as much as possible.

Jan's qualifications are listed below:

- ✓ Master of Networking and Sys admin
- ✓ GAICD (Graduate of the Australia institute of company directors)
- ✓ BTEC - Electronic engineering
- ✓ ISO 2000 certified consultant
- ✓ Prince2 certified project manager
- ✓ ITIL certified
- ✓ MCSE (Microsoft certified systems engineer)
- ✓ CLP (certified Lotus professional)
- ✓ JNCIA-FW / SSL / WX (Juniper networks certified Internet associate)
- ✓ CNA (certified Novel administrator)

It Could Never Happen To Me

Statistics from the USA show that 65% of business under 200 seats have inadequate or no backup at all. We all know that statistics can prove anything, however after working with numerous businesses in the Melbourne area over the last 14 years, we have found that at least 95% of businesses do **NOT** have reliable backup of their data and do **NOT** know how or what they would do in the event of a disaster. They simply *“hope”* that their backup is/was working and that it will save their bacon if a disaster strikes. This *“hope”* approach is implausible 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. It is similar to not having insurance, so you take all the risk, which is not a position good business people would like to be in.

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 in the US that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for insolvency immediately (Source:).

The following, are some other statistics about losing data:

Every piece of hardware and every piece of software can be recovered or replaced in the event of a disaster, but if the data is lost it is lost forever. Years of intellectual property, documents, correspondence and records are almost impossible to recreate in a reasonable time frame, and no insurance payout will make it any easier.

Did you know?

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.

If you're using External USB Drives to back up, the majority only provide a short warranty time - sooner or later they will fail.

The latest Kroll On track survey (April, 2010) of Australian IT professionals showed that:

- 50% of Australian companies don't check that backups succeeded.
- 10% of IT managers test the success of their backups annually.
- Only one third of organisations (39 per cent) sporadically check that their backups work. Some never tested the backups at all
- 20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. (Source: Richmond House Group)

Gartner estimates that only 35 percent of Small and Medium Sized Businesses (SMBs) have a comprehensive disaster recovery plan in place (our experience has found that number to be much lower)

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)

9 Critical Characteristics to Demand for your Backup and Disaster recovery system

So what should you look for when choosing a company or product 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?

There are two critical metrics to consider with backups and disaster recovery

Firstly, RTO (recovery time objectives) how long it takes to get your data back/system operational again

Secondly, RPO (Recovery point objectives) how long since the last backup

In the ideal world you want these numbers to be as close to zero as possible

Unfortunately, finding the right system for your business 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 in the first place, leaving you high and dry when you need it most.

Here are 9 things we recommend looking for:

1. To have the ability to recover Normal Business Operations FAST. There is only one question to ask! "If my server crashes beyond repair, how long do I have wait to be operational again?" You do NOT want to have your expensive staff waiting idly around for the new hardware and then the data recovery to take place. Also, the longer you are off the air, the worse your business credibility.
2. When backing up, there should be no requirement for manual human intervention (unless there is a fault) relying on a person to change tapes, disk drives will almost guarantee that at some point it will not get done. **The system has to be fully automatic.**
3. Frequent daily backups: Another feature to look for is ongoing daily backups versus a nightly backup. This allows you to restore a file that you worked all morning on and saved shortly before the server crashed in the late afternoon.
4. Make sure your data is encrypted; it is being transferred over the Internet and stored in a location outside of your office. It should be encrypted to a level that even the vendors cannot access it, without a passkey or passphrase.
5. The ability to "virtualize" your server. This is a fancy term for putting your server online so that you and your staff can work even if your server has had catastrophic failure.

6. Demand file versioning or historical backups. In the days of tape backups when a proper tape rotation was used, it would be possible to go back to a specific version of a file from different time periods.
In other words it is possible to restore a spread sheet you worked on last night and three weeks ago. Most online backup services only back up the last version of a file; so make sure you choose one that features file versioning or has the ability to access historical backups
7. Offsite internet backups to an Industry-Grade Data Centre (the cloud). One of the first things you need to ask your IT person is, "Where will my data be stored?" 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 Centre. A TRUE data Centre will be 100% dedicated to hosting data and should have:
 - Redundant power sources, generators with on-site diesel tanks
 - Fire Detection and Suppressions systems
 - High-level, 24 X 7 on-site building security
 - Redundant Internet access which has multiple carriers
 - Sophisticated Building Management Systems
8. 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 a "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 that no one responds to.
9. 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.

Want to Know For Sure If your Data Backup Is Truly Keeping Your Data Secure?

Our Free Backup and Disaster Recovery Audit will reveal the truth

If you are worried about whether or not your current backup and disaster recovery processes are working as you think they are, I'd like to offer you a **Free** backup Audit (\$500 value) as a means for introducing our services to your business.

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 to your office

- Audit your current data backups, including 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 that is overlooked.)
- Provide a report showing your current RTO and RPO (how long to recovery and how much data you will lose)
- Answer any questions you have about backing up and securing your data. We're also happy to put together more than one option for backup and DR 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.

We will provide a gap analysis of your current data backup system and if it's appropriate, we'll provide you with options to make your data more secure.

Naturally, I don't expect everyone to become a client. However, 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 obligation free backup and disaster recovery audit

You can request this, simply by doing one of the following:

1. Call our office on 1300 501 677
2. Email support@mspblueshift.com.au
3. Online at www.mspblueshift.com.au