# Back up your data

One day **it could save your business**

BOLD-ICT

***It's Friday evening, you've shut up the office and you're all done for the weekend. Time to head home.***

*As you're eating your pasta, the phone rings. And it's the call no business owner wants to get.*

*When you arrive back at the office, firefighters are hosing down the last of the flames and you're dialling your insurers. It's not a disaster, but your server room is toast.*

*A few days of clean-up, some new kit and air freshener and all will be shipshape again, ready to restore everything from your backup.*

***You are all backed up... Right?***

*Fire, theft, accidental file deletion or disgruntled employees... there are lots of reasons why you might need to rely on your backup system.*

*But the most likely reason by far is that your business becomes the victim of a cyber crime.*

*There are countless forms of criminal attack, many of them designed to steal your data and either encrypt it or deny you access to it until you pay a ransom.*

*This kind of crime doesn't have to trigger a full scale disaster, but it's a fact that most small businesses that are hit with a full-on cyber attack don't recover from it.*

*For all these reasons, backing up your data is one of the strongest precautions you can take. Set it up properly and make it part of your routine to check that it's working. Because one day your backup could save your business.*

**Here's what you need to know.**

## What exactly is a data backup?

Backing up involves creating a copy of your current data that you can call upon should your original files become corrupted, stolen, lost or accidentally deleted.

If you lost all your business data tomorrow, what would you do? You couldn't contact clients, you'd have no projects available, no staff records and no information about your products and services. That's not to mention your financial data, invoicing status… the list goes on.

It can be catastrophic. Almost 70% of small businesses close within a year of suffering a large data loss.

And 94% of businesses that experience severe loss of data never recover. **Let that sink in for a moment.**

That's why it's so worrying just how many devices aren't being backed up properly in a typical company, and how many businesses don't take enough care of their data.

So if you don't want to risk becoming a statistic, you need to take data backup seriously. That means having a strategy and a robust solution in place.

## What data should be backed up?

Every business should back up files and documents containing financial data such as invoices and bills, statements, payable files, and payroll. You should back up customer data, supplier information, partner information, communications and email accounts, as well as all your applications and databases, your project management files, personnel records, operating systems, configuration files… and any other files you or your team create.

Don't forget mobile devices. Phones and tablets used for work have the potential to hold even more sensitive data than a laptop.

That makes it important to review your scope anytime you make changes to your infrastructure, or whenever you add devices, solutions or services.

If you have the capacity, it's a good idea to appoint a Backup Administrator. It becomes part of this person's job to handle your backup strategy, including the tools and solutions you'll use, the scope of the backup, the network and storage, as well as your Recovery Time Objectives and Recovery Point Objectives (more on those later).

In a small team this may be a lot to expect from a colleague who isn't a tech expert, and many small businesses choose to outsource this to an IT support professional. **That's absolutely a service we offer, so get in touch if you'd like to discuss it.**

# How often should you backup?

## Everything. Every day. At least.

Your backup schedule has to work for the amount of data you and your team process in any given period. That's because, in the event of a disaster, you'd lose any data created between the last backup and the point of failure. **This is called the Recovery Point Objective (RPO).**

If yours is a business that processes a lot of data, daily backup might not be enough. A shorter RPO means losing less data, but requires more storage capacity, and more network resources. That comes at a cost.

Longer RPOs are more affordable but mean risking the loss of more data.

While most small businesses define a backup period of 24 hours, it's possible to create tiered RPOs, where critical systems are backed up more frequently, and secondary systems have a longer RPO.

Another important factor is your **Recovery Time Objective (RTO).** That's the amount of time it takes to recover your data from the point of failure. You know that when your systems are down your company loses money, so it's important to recover quickly to minimise your loss.

**Just like RPO, a shorter RTO requires faster storage and technologies. And unsurprisingly, that costs more. For most companies, a few hours is normal.**

# How do you choose a solution?

There's a huge choice of backup solutions and tools. Finding the right one for your business may take some thought, but if you've considered your scope, your RPOs, and RTOs, you should have a better understanding of which way to go.

## These are the most popular solutions available right now:

**Hardware appliances**
This is a physical device that includes pre-installed backup software and storage, and usually comes with all components integrated. That makes it easy to set up and configure. You can access it through its own interface on your computer.

Keep in mind that if this type of appliance fails, you lose your entire backup solution. Even if you have a secondary backup, you need to replace your hardware appliance before you can access data – which increases recovery time.

**Software solutions**
These are installed on your existing system and allow you to back up to a destination within your current network (although it's often best to have a dedicated backup server).

You'll need to install and configure the operating software but, compared to hardware appliances, software solutions give you greater flexibility. They can also be less expensive.

**Cloud services**
Perhaps the simplest solution, cloud services – also known as Backup as a Service (BaaS) – let you run your backup directly from the cloud. You need to install some software on your local devices but you don't need additional servers or systems. It also makes it simple to scale up the storage you need as your business grows.

Remember that if your business handles a lot of sensitive data, you'll need to make sure your chosen provider adheres to the relevant data protection legislation and that the right security protections are in place.

**Hybrid solutions**
It's become common to combine local with cloud backups, creating a very robust hybrid solution. It brings together the best of both worlds, which makes it a popular choice.

## As easy as 3-2-1

**A hybrid solution is one good option that also follows the strong, industry accepted 3-2-1 approach.**

Store your data in 3 places
Using 2 types of storage
With 1 copy stored off-site

## What type of backup should you choose?

**There are three types of backup that each work slightly differently, at different speeds and with different advantages.**

**Full backup**
This makes a copy of everything you want to protect. The first time you perform a backup you'll want to do a full backup which can take many hours.

**Differential, aka cumulative incremental backup**
Once you've completed a full backup for the first time, you may switch to a differential backup. This only backs up files that have changed since the last full backup. These are faster because less data is being copied, however
the amount of data grows with each differential backup, until the next full backup.

**Incremental backup**
Again, these only copy changed data, but they copy what's changed since the last incremental or full backup. These are much smaller and faster because new data is being copied over daily. The less time between backups, the smaller the amount of data to be backed up. With more sophisticated software you can back up every hour – or even more often.

On the downside, this type of backup may take longer to restore because the data has to be assembled from the last full backup and every incremental backup since then.

# What storage do you need?

**Your backup needs to live somewhere.**

**Local or USB disks**
If you have the storage capacity, you could back up individual machines to local disks, or to an external USB drive.

It's fast and you don't need a network. However, if your device was damaged – in a fire, for example – your backup could well be destroyed alongside it. It may also mean that you have to manage your backups device-by-device which is inconvenient, especially in bigger companies.

**Network shares**
NAS (Network Attached Storage), SAN (Storage Area Network), or even just a simple folder on your network, lets you store all your company backups in one place, and restore whatever you need, when you need it. However, as with local disks, if you suffer a major disaster your backup may be lost too.

**Tapes**
If you're concerned about fire, flood, or equipment theft, a sensible solution is to have a backup stored off-site – ideally 100+ miles away from your data centre.

A traditional way of doing this is to copy data onto tapes and physically ship them to a distant location. Modern tape technology stores a large amount of compressed data.

This may not feel very 21st century, but tapes are a robust way of storing and archiving data for a long time – 30 years or more. As you can imagine, though, recovery could take time. You can restore entire systems this way, but it's impractical for single files.

**Cloud storage**
A fast internet connection allows you to send your backup files to the cloud. You subscribe to the storage capacity you need and can easily add more without having to invest in hardware. To avoid issues with uploading large volumes of data, cloud storage suppliers may also offer physical data shipping or one-off initial 'seeding' systems which avoid a massive first upload.

## Talk to us

**Different solutions come with different benefits and drawbacks. To decide which is right for you, you need to look at all your individual requirements, your RPOs, and RTOs and the resource you have to maintain a system.**

There's a lot to think about and a lot of information to gather before you commit, but it's a vital precaution that every business should take.

**We implement backup and recovery solutions every day. To speak with an expert, get in touch.**

**CALL:** 03 5410 8999
**EMAIL:** hello@bold-ict.com.au
**WEBSITE:** www.bold-ict.com.au

BOLD-ICT