



ab
01

Disaster Recovery:

The Active Business Series

Business Resilience



If a disaster were to strike your business could you maintain essential operations during the emergency and fully recover afterwards?

The commonest threat to a business is data loss, but there are many other potential threats such as sudden loss of key staff, unexpected loss of a critical supplier, or disruption to essential services such as electricity, not to mention possible disasters such as a fire, storm, flood, or even a terrorist attack.

Being unprepared for such eventualities could be severely damaging and potentially fatal for a business. A little time and energy spent now developing a business continuity plan could prove to be a very worthwhile investment in the future.

If you would like to discuss how we can help you with a business continuity plan, give us a call today.

How safe is your data?

Unfortunately, data loss is very common in the business world. It may occur as a result of a systems failure, human error, criminal activity, or some form of natural disaster.

Besides the immediate disruption to your business operations there can also be a long term financial impact and even serious legal consequences if certain types of data fall into the wrong hands.

There are basic precautions you can take to protect your data:

- Decide what data is critical - for example your accounts, customer details, VAT returns, contact list, product information, etc - and implement an appropriate daily or weekly back up cycle
- Arrange secure off-site back up for critical data
- Store valuable documents etc that cannot be backed up in a secure fire proof location
- Ensure you have all the latest software patches, anti virus protection, and other security measures installed throughout your IT system
- Make sure sensitive data can be accessed only by authorised personnel

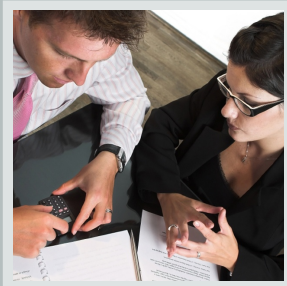
You might consider taking advantage of the increasingly sophisticated cloud computing facilities for some of your critical functions. Not only will this give you secure off-site back up for all your key data and documentation it will also enable you to access your records and carry out critical functions remotely - and from multiple locations.

Data - the weakest link



- Only one in a hundred businesses back up their data daily
- Over half of data back ups are incomplete
- Half of all attempts to restore data are unsuccessful

Why you need a business continuity plan



Besides protecting and backing up your data, it is wise to have a general business continuity plan that will help you maintain critical functions in the event of any major disruption and quickly recover normal operations once the crisis has passed.

These days there is a growing expectation for businesses to have a continuity plan in place. Almost two thirds of businesses are now required by customers to show they have one and nearly three quarters of businesses require the same of their suppliers.

A well formed plan has a number of advantages:

- It gives your business resilience - the ability to adapt and survive in difficult circumstances
- It can strengthen your brand, enhance your reputation, and help you win and retain customers
- In some industries, tested recovery procedures are a legal requirement and failure to demonstrate them can lead to heavy fines
- In certain circumstances a good plan can result in lower insurance premiums



Did you know ?

- Nearly 1 in 5 businesses suffer a major disruption every year
- 80% of businesses affected by a major incident close within eighteen months
- 90% of businesses that lose data during a disaster close within two years

Preparing a plan for your business



To prepare a continuity plan for your business you will need to assess potential risks of disruption to your core products or services, establish the minimal level of operation that must be maintained, prepare contingencies to maintain these levels during an incident, and have plans to fully restore operations once the incident has passed.

Needs will vary from business to business but most organisations will need to address the following:

- Do you have back up plans in the event of key staff being unavailable?
- Have you made sure you have no single points of failure among your staff?
- Should your premises become unusable could you transfer operations to an alternative location?
- If alternative premises are not available, do you have arrangements for employees to work remotely but still be able to contact customers, suppliers, and other employees?
- Have you checked with your regular suppliers to see if they have continuity plans and discussed contingencies with them?
- Have you identified alternatives in case any of your regular suppliers fail?
- Do you have easily accessible off site back ups of all your essential records?
- If your IT system is damaged or compromised, say by a virus, do you have access to an alternative system for the duration?

This is just a brief look at some of the issues involved. If you would like to examine the matter in more depth, please call. We would be happy to help.