

Business Continuity Planning

Is your business prepared for the worst? Any business can experience a major emergency - so what can you do about it?

Any business can experience a major emergency – such as flooding, severe weather from blizzards to heat waves, flu epidemics and terrorism – or serious incident – fire, explosion, loss of power and loss of personnel – that prevents it from continuing normal operations..

You have invested heavily in your business and you need to ensure it remains safe, secure and viable.

Therefore, it is most important for your business to be prepared for all eventualities and to have a plan in place to enable it to return to normal as quickly as possible. It will reassure your customers and suppliers that you take the resilience and security of your business seriously and is good business practice. Also, small firms tendering for work with large organisations, including Local Authorities, could come under increasing pressure to demonstrate their own preparedness.

A Business Continuity Plan describes the practical steps your business needs to follow if a particular problem arises. The planning process will involve:

- Identifying potential disasters or emergencies
- Looking at how you can minimise risks
- Deciding how you intend to react to eventualities

Why do I need a plan?

If you have a Continuity Plan in place, you will be better prepared to cope in a crisis and should be able to minimise disruption to both your business and your customers.

It will ensure that staff know their roles and responsibilities and respond by following recognised, practised and agreed procedures.

The most important functions, services and systems that are essential to running your business will be up and running in the shortest possible time frame. The impact on your business will be limited.

Need to know more?

For more information contact Colin Bailey or Andrew Milverton on 0118 940 6175 at Cassey Miller James.

Details of our offices and telephone numbers can be found on our website at www.cmj.co.uk



Assessing the risks

It is important to identify the risks to the most critical aspects of your business.

List the potentially serious incidents or points of failure that could affect your business and assess how each particular occurrence may affect the business. This will help you to determine what you would need to do if one of these things actually happened.

To decide what impact an event might have on your business think about some worst-case scenarios and how they might affect you.

What would happen if your premises were destroyed by fire? How would an explosion or fire in your neighbours' premises affect your daily operations?

If you lost all the information you held on customers through a computer virus, how would you recover the information and how would you contact your customers?

If your staff rely on public transport to get to work, what would you do if the station was closed or the roads blocked by severe weather or due to a terrorist attack?

What would happen if there was a sudden and continuous power failure; how would you operate machinery or be able to see?

What if you lost key staff, through death or sudden illness?

What if there was a break in your supply chain e.g. a key supplier going out of business?

What should your plan contain?

If your business is large enough, form a disaster recovery team who will have responsibility for developing and implementing your Continuity Plan, but assign overall responsibility for the Plan to one member of staff. That person would be responsible for recording the Plan, testing and ensuring it is kept up to date.

The plan should include:

- Immediate actions to be taken, e.g. contacting emergency services and key members of staff
- Which business functions you need to get 'up and running' as a priority and how this will be achieved
- What resources you will need to get these priority functions operating • What each individual's role will be if there is a disaster or emergency. Who will deal with any media enquiries? Who will deal with the insurers?
- Details of alternative premises to be used – make reciprocal arrangements with other local businesses to share premises temporarily.
- Details of where and how key data and information is backed up and instructions for how to access those back-ups
- Contact details of those who need to be notified, e.g. insurance companies, customers, suppliers, utilities providers etc
- Details of service providers who can help, e.g. plumbers, electricians etc
- A map of the layout of your premises to help the emergency services

The Plan should be in writing and kept securely. It can be retained on the premises but there should also be a copy kept away from the premises, e.g. at the home of a senior employee or at the Bank or Solicitors. A checklist approach will be helpful as key steps can be easily identified and this will enable you to tick things off once they have been done. Make sure that all staff are aware of and familiar with the Plan.

Testing your Plan

Disaster Recovery Plans should be tested on a regular basis, which could involve a simple paper exercise, including a run-through by the people involved.

The Plan should be in the right order so that your business can be up and running as quickly as possible.

Check the contact details contained in the plan regularly to ensure they are correct.

A full test may involve a simulation of an emergency. Record the procedures and results of the plan and use this to review and fine tune the plan if necessary.

If your plan is ever invoked to contend with a real incident, learn as much as you can from the experience and refine your plan to reflect where you think improvements could be made.

Minimising the risk

There are several things you can do to prevent disasters occurring in the first place, or to minimise their impact:

- Make health and safety a priority
- Make sure there is a qualified first-aider
- Install fire and security alarms
- Keep paper documents in metal cabinets to minimise fire damage
- Keep copies of irreplaceable documents away from the premises
- Protect IT systems with antivirus software, keeping back-up data away from your premises
- Keep records of your business systems and procedures

Why bother?

Disasters have no boundaries and whether you are a small or large business you may be affected.

Research has shown that around 80% of businesses that suffer a disaster such as loss of computer data, damage caused by flood, fire or a major incident, cease trading within 12 months of the disaster.

Without an effective continuity plan your business could suffer from:

- Loss of trade
- Damage to image/reputation/brand
- Loss of customers
- Loss of staff
- Loss or damage to equipment and/ or premises
- Impact on insurance premiums

With no recovery plan your business has less chance of survival therefore, the time spent in putting together a business continuity plan is good for your business, staff and reputation.

The Civil Contingencies Act 2005 placed a duty on Local Authorities to provide advice and assistance to local businesses and voluntary organisations.