AVIVA

Recover or Fail?

Business Continuity Planning for Technology Risks

Introducing Business Continuity Planning

Introduction

Technology is a highly competitive industry and if a business suffers a major loss they may be unable to meet the supply requirements of their customers.

A key factor to a business recovering quickly from a major disaster such as a fire or terrorism event is whether or not the business has a Business Continuity Plan (BCP) in place. Of course, you may never need to use this, but if the worst does happen, it may be the difference between your business recovering or failing.

To address this, we've produced Guidance Notes and a Planning Template to assist our technology sector policyholders. By following our guidance you should be able to create a BCP which, in combination with the correct insurance cover, will help your business survive and recover.

Benefits of a BCP

1. Significantly increases the chances of your business surviving a major incident.

2. Insurance plays its part, but many of the effects of a disaster such as damage to your brand or reputation may not be insurable.

3. Without a BCP in place, it is difficult to be sure that your Business Interruption insurance period of cover is set long enough for your profits to return to pre-incident levels.

4. Large customers may ask for evidence of such a plan as part of contract negotiations.

5. Provides evidence of good risk management which could improve your overall insurance deal.

Overview of the process

Business Continuity Planning is important for organisations of all sizes because at its most fundamental level it seeks to:

- Minimise the chance of the business suffering an incident which damages or disrupts your business

- Maximise the ability of the business to recover from an incident and continue trading.

We believe that Technology businesses can significantly benefit from preparing a BCP, but we also recognise that your time is precious. So to help you understand the process, we've broken it down into 5 simple stages.

It's often easier to understand what you need to do by looking at what someone else has done, so we've included a series of examples for a hypothetical company, The Green Electronics Product Co., shown in green shaded areas.

The Green Electronics Product Co. designs and manufactures industrial processing control equipment and is based in Cambridgeshire. It buys in electronic components and plastic casings. It uses highly automated machinery for printing and populating circuit boards, and finally bench assembling these into the casings. It has contracts to supply bespoke control panels to UK and European-based companies, which account for 75% of turnover. Additionally, it manufactures a standard electronic timer component which it regularly supplies from stock to two UK-based manufacturers and to a variety of other customers on an ad hoc basis.

Further hints and tips on Business Continuity Planning for technology companies are shown in yellow shaded areas.

Please note that:

- We have a policyholder Risk Helpline which can provide guidance on your risk management needs. Call us on 0845 366 66 66 (open Monday – Friday 9am – 5pm)

- Once you have completed this template for your business it's important to keep a copy off site with your computer/business records and ensure your employees know where to locate it

- This BCP is aimed at smaller single site businesses and deliberately focuses on the basic fundamentals in order to remain as concise as possible

- For larger multi-site businesses Aviva can supply a more comprehensive BCP template

- Aviva Risk Management Solutions provides a range of training focused on Business Continuity Planning. Contact us on the Helpline number above or visit www.aviva.co.uk/risksolutions/

Guidance notes: How to prepare your BCP

Stage 1 – Service levels

This stage is about documenting what your business does – and must continue to do – in order to operate effectively.

- Normal Service Levels
  - What does your business routinely aim to deliver to your customers in terms of product and timescales?
  - This will allow you to record what is important to your business before any incidents occur and have a target for the business to recover to.
  - Think about your business targets and what outputs are required to ensure these targets are delivered. In simple terms this is what the business exists to do on a day-to-day basis.
  - Remember to include any specialist areas or processes.

- Minimum Service Levels
  - What is the minimum service level required to fulfil main contracts and keep important customers and to avoid permanent loss of custom?
  - This is the basic service you will need to continue to deliver to ensure your business survival.
  - Ask yourself if you need to continue with any specialist services or processes or if you can introduce acceptable alternatives.

- Maximum Downtime
  - How long will your customers tolerate an interruption to your service before taking their business elsewhere?
  - How soon until your market reputation is damaged?

Normal Service Level for the Green Electronics Product Co. is to batch manufacture its bespoke products and supply these to pre-agreed schedules from storage in a third party warehouse. Standard products are produced evenly throughout the year and held on-call in their on-site warehouse.

Minimum Service Level for the Green Electronics Products Co. is to ensure that all contracts to supply bespoke products are honoured.

N.B. Whilst it is desirable to supply the standard products as well, this may not be possible following a disaster as capacity will inevitably be limited. The business believes it will be easier to recover custom for standard products than bespoke products.

Maximum Downtime for the Green Electronic Products Co. is 4 weeks. This is because most customers have 4 weeks' product in stock. A couple of smaller customers only retain 2 weeks' stock but will tolerate a further 2 weeks' disruption.

Stage 2 – Risk assessment

This stage involves:

- Identifying the key threats facing your business, e.g. fire, food, machine breakdown etc.
- Deciding on measures which would minimise the likelihood of these threats occurring.
- Deciding which of these measures are practical to implement and over what period of time.

Some examples of measures which could potentially be taken to reduce the risk of threats occurring are:

Fire
- Undertaking a Fire Risk Assessment to comply with your statutory responsibilities.
- Ensuring flammable supplies/materials are stored away from fire inception hazards.
- Regular maintenance and inspections of fixed electrics.
- Providing a fire resistant cabinet to store high value reel components with long lead times.

Flood
- Storing supplies/products off the floor, e.g. on pallets.
- Pay particular attention to where you store hazardous materials (e.g. inks, solvents and oils) which may contaminate flood waters.
- Relocate vulnerable equipment to other parts of the premises.

Security, Arson and Theft
- Improving security measures to prevent arson/theft such as security alarm and perimeter fencing.

IT Measures
- Keep your anti-virus software up to date.
- Consider a UPS (uninterruptible power supply) system to ensure safe shutdown following a power failure.

Stage 3 – Incident Management Planning

The next stage is to put a plan in place to help your business cope with the initial period after an incident.

Of course, the welfare of your staff and visitors to the site will be your first priority.

After that has been taken care of you can turn your attention to your business. Pre-planned actions taken in the immediate aftermath of the incident can have a big impact on the subsequent speed of recovery for your business.

There are three areas you will need to cover:

- Implement damage limitation measures especially relating to security, avoiding further damage (e.g. by weather causing further damage to weakened property) and the salvage and removal of machinery and contents.
- Make contact with those who can help and those who need to know about the incident. You may not have access to your usual company records and contact directories after an incident. Think about who you'll need to contact and record their details in your business continuity documentation.
- Stabilise your business at the Minimum Service Level you have already defined. Now you need to think about the short-term measures and temporary work-arounds you can undertake to enable you to return to delivering your minimum service level.
- Make contact with our claims service and your broker.

Short-term measures and temporary work-around options for the Green Electronic Products Co. include:

- To utilise the stock of bespoke products which is kept in the third party warehouse
- To utilise stock of standard products in own warehouse (if unaffected by the incident)
- Subcontract the circuit board manufacture work to a mutual assistance partner (see note below) to meet service level agreements when this cannot be met by own capacity. An agreement has been reached with a contract electronics manufacturer, which they already use from time to time, to undertake work for them (thus ensuring quality standards are met)
- Retain own final bench assembly where possible.

To address these areas your BCP needs to include:

- A list of Emergency Contacts
- A list of Immediate Actions required to limit disruption following major loss, e.g. fire, flood etc
- A list of actions required to address disruptions to specific activities, e.g. arranging subcontracting.

Battle Box: To ensure you have all the resources you will need, you should prepare a 'battle box' of items that will help manage the incident and complete your first actions. Carefully consider where you'll keep your battle box. It must be in a location that's secure but also accessible. Examples of what you might want to include in your battle box are:

- A copy of your Fire Risk Assessment
- A copy of your BCP
- Asset register and inventories
- Company stationery and letterhead
- General stationery and writing materials
- Data restoration instruction
- Disposable camera
- Yellow Pages/local directory
- Insurance documents.

Stage 4 – Business Recovery Planning

Once you've stabilised your business at delivering its minimum service level, you'll need to move forward. Firstly you must establish how quick the physical recovery will be. If the premises and machinery will be repaired quickly then you may not need to take further action other than preparing to 'hit the ground running' once the repairs have been completed.

Your customers are unlikely to wait for an extended period and will move to other suppliers if you don't take action to restore your normal service. You'll need to think about issues such as:

- Implementing alternative working practices such as subcontracting
- Identifying and equipping temporary premises perhaps using second-hand machinery and bringing as much work back in-house as possible
- Monitoring the progress of the reinstatement work at the damaged premises, ensuring that this goes to plan and that machinery etc. is ordered, installed and commissioned at the appropriate time
- Keeping in contact with customers and trying to win back the lost business as capacity improves.

Some areas for consideration which could potentially maximise the chances of your business recovering following a major incident are outlined in the BCP Template on page 6.

Business Recovery Actions for the Green Electronic Products Co. include:

- Continue subcontracting circuit board work to their mutual assistance partner
- If longer disruption is likely, relocate the business to temporary leased industrial premises
- Consider what machinery, perhaps second-hand, can be installed in the temporary premises and what changes to working practices would be required
- Consider staffing levels required, e.g. overtime, temporary/agency staff
- Order new automated circuit board manufacturing machinery
- Decide at the time whether to reinstate machinery at temporary premises or subcontract until own premises are ready to re-occupy.

Mutual Assistance Partnerships: Some firms will find it beneficial to enter into mutual assistance partnerships with other businesses where you agree to help each other cope with a major incident. When approaching other firms, be prepared for a two-way discussion around the assistance you can give them as well as the assistance you may need. Any assistance will be subject to capacity constraints at the time of the incident so you may want to set up several partnerships, especially if you have specialised processes. You may already subcontract some work during your busy periods and you might want to consider approaching those firms. Otherwise, your Trade Body may be able to assist you in identifying suitable firms to approach. Remember to discuss the associated costs with your insurer.

N.B. When subcontracting is used it is essential to ensure that quality standards are observed. Also, be aware of the risk of subcontractors 'poaching' contracts. Retaining control of client contact and final dispatch can help to mitigate this risk.

Stage 5 –
Plan Rehearsal and Maintenance

Rehearsal: The first stage is to ensure you – and anyone in your business that will have a key role in assisting you – are familiar with the plan and its contents. Plan some time when you can read through the plan without distractions and ensure that it all makes sense to you.

The next stage is to run a desktop rehearsal. This will also involve getting together with those in your business who will have a key role in assisting you. You can agree on some 'what if' questions and see if the plan can be used to assist you in dealing with the incident. For example you might want to ask "what if we had a fire?" Does the plan have enough information to allow you to deal with the incident?

If you uncover uncertainties during this exercise, then your BCP probably requires further work.

Maintenance: The objective of maintaining your plan is to ensure that the data and contact details are up to date. You'll find it difficult to use your BCP if these details are out of date. So it's important to regularly maintain the plan data and contact details (this needs to be done more often than plan rehearsals).

Aviva Risk Management Solutions can provide assistance on plan rehearsal and maintenance. You'll find their contact details on page 2.

The Green Electronic Products Co. undertook a phased Plan Rehearsal. The first stage was to have everybody involved read over the plan individually and this resulted in several improvements being made and details changed. The next stage was to get everyone together for a couple of hours to talk through the recovery options. This resulted in one person being given the task of reviewing and maintaining the contact details and plan data (including customer details, machinery lead times and availability of subcontractors) on a 6-monthly basis. The group agreed to reconvene in a year's time to talk through the recovery options again and confirm if they were still valid in the light of changes to the business and customer base since the plan was first written.

Technology Risks Business Continuity Plan (BCP) – Template

N.B. Existing boxed text may be typed over

Business Continuity Plan for

Date plan issued: _____ Ensure all previously issued versions are destroyed.

Business Continuity team member	Role/Position	Contact details

Stage 1: Service Levels

Service Levels	
My normal service level is:	
My minimum service level is:	
My maximum downtime is:	

Remember to include details of any major customers with more specific service level requirements such as:

Customer name	Value of contract	Normal Service Level considerations	Minimum Service Level considerations

Stage 2: Risk Assessment

Threat	I can reduce likelihood by…	Implementation target date	Done

Technology Risks Business Continuity Plan (BCP) – Template (continued)

Stage 3: Incident Management Planning

Remember the first priority is to ensure the safety and welfare of all staff and visitors.

Location/Address	
Contact details	
Battle box location	

Immediate Damage Limitation Measures: Security, Weather Protection and Salvage – record the measures you will consider deploying in the event of an emergency.

Issue: what's gone wrong	Measure: what to do about it	Supplier: who can help
Record the contact details for all suppliers in the contact lists below		

Major Incident Management Actions (amend as appropriate)

Action	Done

Return to Minimum Service Level

My general strategy to return to providing minimum service level is:

My (optional) detailed strategy to implement this is:

Disrupted activity: what's gone wrong	Action: what to do about it (temporary work-around)	Provider: who can help
Record the contact details for all suppliers in the contact lists below		

Stage 4: Business Recovery Planning

Return to Normal Service Level

My general strategy to return to providing normal service level is:

My (optional) detailed strategy to implement this is detailed below:

Disrupted activity: what's gone wrong	Action: what to do about it (temporary work-around)	Provider: who can help
Record the contact details for all suppliers in the contact lists below		

Maximising your business recovery (Potential issues to consider below)

Issue	Recovery action to be taken	Implementation target date	Done

Stage 5: Rehearsal and Maintenance

Rehearsal
The last plan rehearsal was carried out on:

The areas where the plan could be improved are recorded below:

Issue raised during rehearsal	Action to be taken to address this	Date for implementation	Done

The next plan rehearsal is due to be completed by:

Maintenance
The last maintenance check on the plan was done on:

The outstanding issues are:

The next maintenance check is to be completed by:

Contacts Appendix

Premises Contact List

Category	Name/Company	Contact details	Comments

Utility Supplier Contact List

Category	Name/Company	Contact details	Comments

Business Services Contact List

Category	Name/Company	Contact details	Comments

Contacts Appendix (continued)

Equipment/Machinery/IT Supplier Contact List

Category	Name/Company	Contact details	Comments

Additional Business Continuity Service Providers Contact List

Category	Name/Company	Contact details	Comments

Further Contacts and Additional Documents

You'll also need to make contact with others such as suppliers, customers and staff. You may also need access to some company documents, e.g. asset register, to help with an insurance claim.

You are likely to already have these details recorded on company systems – however you may not have access to these systems following an incident. So it's best to print off these lists and attach them to your plan. Make sure you include relevant details such as your reference numbers for suppliers and customers as well as next of kin details for staff.

Further Contacts/Additional Documents			
The additional documents appended to this plan are (e.g. staff contact list, asset register):			

Contacts Appendix (continued)

Business Continuity Log: for use if the plan is invoked

Use this log to record:

• The actions taken

• The decisions taken

• Any information obtained during the incident

• Any expense that has been incurred.

This will help you to keep track of the incident and also to prepare any insurance claim.

Date/Time	Record of action/decision/information	Expense incurred	Logged by