



Business Continuity Planning – What are the current challenges and what should businesses be doing

By Robert Mackenzie, Partner, Business Technology and Consulting, Scott-Moncrieff

Planning for recovery from a major incident or disruption is increasingly recognised as an essential component of an organisation's risk management strategy.

Business organisations are accustomed to planning for other areas of risk, so planning for business continuity should be no different. Unfortunately, this is not always the case.

The reasons should be clear:

- Nearly one in five businesses suffers from a major disruption every year.
- 80% of businesses affected by a major incident close within 18 months.
- 90% of businesses that lose data are forced to stop trading within two years.

The risks of serious business disruption are steadily increasing due to the greater complexity of modern business and the burgeoning range of potential threats. An ever increasing majority of those incidents involve the organisations ICT infrastructure as more and more business processes become dependent on ICT. For example, the recent loss of Tesco's tills system resulted in the closure of a large number of stores. Without their IT systems they couldn't do something as basic as take money from people for their shopping.

Business Continuity Planning (BCP) allows management to anticipate such risks and to develop contingency plans to ensure that the business continues to operate whatever the disruption.

The steps a business needs to take are quite straightforward:

- Complete a threat and vulnerability matrix to help you to examine the threats facing your business and develop scenarios of how the threats might materialise.
- Develop action plans to help you to respond to the identified scenarios.
- Link action plans to resources, people, facilities and infrastructure.
- Develop supporting procedures and establish your crisis management team.

Businesses need to delegate prime responsibility to key managers for creating these plans or bringing them up to date and confirming their effectiveness.

Their key purpose will be in guiding each part of the business on how to respond to a disaster scenario. They must hold the essential data and decision criteria staff and managers will need to use when responding to events.

These consistent principles apply to the ICT department as much as to any other part of the business. In fact, my experience is that ICT are often leading the field and have the challenge of setting best practice for the rest of the business to follow. This is often due to the fact that without corresponding BCPs for the rest of the business it is very difficult for ICT to prioritise the recovery of key business systems.

The current volatile business environment is throwing up new business models and new challenges on a regular basis.

The move to cloud computing solutions may increase resilience and reduce costs, but is passing some of your risk exposure to another body, which will put their survival, or that of their highest paying customers, before yours.

Every new significant change in the business environment presents new risks and, hopefully, raises the profile of the need for good and efficient BCP. These range from fluctuations in the oil price, the recession, loss of suppliers, or dependency on key new skills.

For many the focus is on resilience to prevent the disaster occurring, which is a very effective way to reduce the likelihood of a risk materialising. However, no matter how good your resilience measures are, life has a way of intervening and devising a set of circumstances that ensure the disaster will still happen. As the sewage workers called out to deal with the flooded drains put it, "S!t happens".

A recent classic example of this which I came across was the failure of a UPS monitor. In a standard power resilience environment, there will be in-line UPS in place to cover for any sudden power fluctuations or loss. These are usually supported by a range of standby generators which will cut in as the UPS battery power declines below a certain level.

The only problem is that these battery powered monitors don't tell the generators to cut in, if the battery is flat.

Resulting in a modern version of "...a horse, a horse, my kingdom for a horse", which reads something like "... a battery, a battery, my data centre for a battery"

This type of situation is not new. Twenty years ago I worked in an ICL mainframe environment (ahhh the nostalgia) where every time the standby generators were powered up they crashed the mainframe. Not the most effective resilience measure.

For a service-providing organisation which may have contractual penalties, this could have disastrous consequences. For want of a £50 battery they could end up with a six figure penalty for lack of availability.

The important lesson from this recent incident is that both customer and supplier had well developed and tested Business Continuity Plans which they were able to implement as soon as their best endeavours at resilience had failed. This meant minimal disruption to core business processes and containment of the impact of the power failure.

The current trend towards cloud computing for many organisations reinforces the need for the business to have robust and tested Business Continuity Plans, as many of the factors which could result in a major disruption are then out with your control.

The recent focus on Swine Flu has certainly helped to capture businesses attention and is the latest driver of many BCP improvement programmes. At time of writing,, the current swine flu outbreak is in the containment stage; however, this is likely to escalate to full pandemic status in the near future and, as a consequence, members of staff, including key IT specialists, are likely to

- Come into contact with people being tested for the virus;
- Come into contact with confirmed cases;
- Be tested themselves for the virus; or
- Become confirmed cases of flu themselves

All of the above options are likely to have a major impact on any business's ability to deliver services to clients, especially if it starts to occur in significant numbers. We have no way of predicting who will be affected or when, including ourselves.

The multiplier effect of losing key IT staff should not be underestimated; they may be the ones who are making home or remote working available for the rest of the staff, thus minimising the impact on the business. Lose the IT staff and you also lose some of the mitigation, exposing the business to greater risk.

If the IT team (or possibly your cloud computing provider) loses a key manager / specialist for two weeks, who can fill in for them and which projects do you cancel / postpone?

The potential downside of a major business interruption in terms of loss of revenue, dissatisfied customers and damaged confidence is considerable, even fatal. Business Continuity Planning helps to significantly reduce the duration of business interruption caused by a crisis because it reduces the time taken to work out how to recover from it.

Business Continuity Planning is a business-wide issue, NOT just an IT issue and the first step is to create an effective company-wide Business Continuity Plan.

Draw up how your business works, what the business areas are and what each area needs to function correctly.

Don't overlook non-IT issues such as buildings, desks, documentation and staff. Then look at the measures already in place to cope with problems, if any, and whether they are enough. Lastly, try to understand the cost of an area not being able to do its job within a certain amount of time. This information will drive everything else.

These are questions that only the individual business can pose and answer. **Now** is always the time to start that process.

Contact:

Robert Mackenzie: robert.mackenzie@scott-moncrieff.com or 0131 473 3500