IT Disaster Recovery ...It's Just the Tip of the Business Continuity Iceberg

The importance of a holistic approach to Business Continuity and the art of making decisions when everyone's under pressure

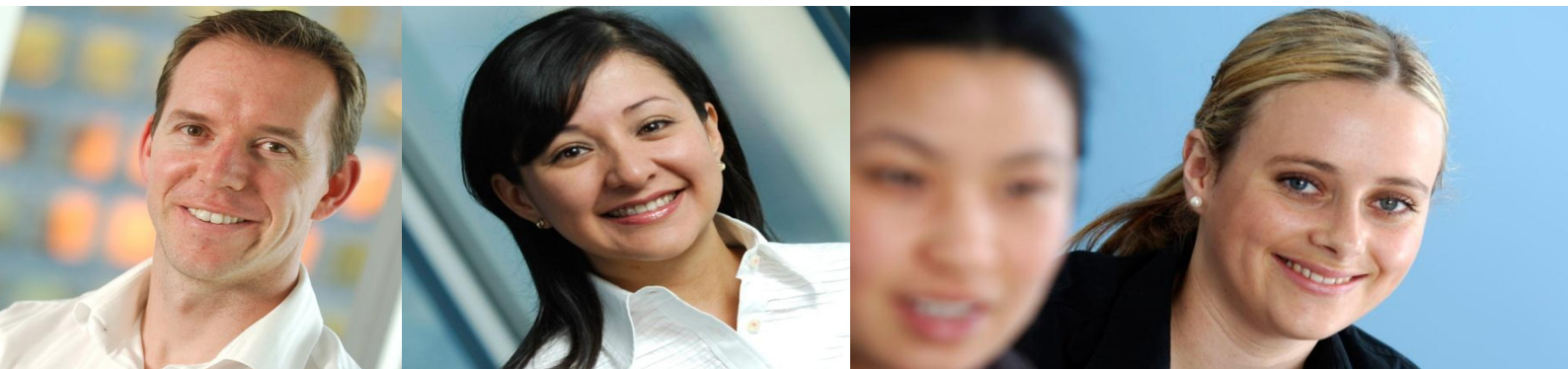*By Professional Advantage and Rinske Geerlings, Managing Director, Business As Usual*

Table of Contents

The importance of a Disaster Recovery strategy

In recent years Australian businesses have become all too aware of the importance of a practical disaster recovery (DR) strategy. Protecting operations against the effects of power outages, human error, natural disasters and an increasing variety of malicious cyber threats has become an essential consideration when establishing an IT infrastructure. As a result, identification of the processes, procedures and assets required to get IT systems back up and running as quickly as possible has become a standard task in the typical IT Manager job description.

- Less than 50% of all organisations have a business continuity plan in place.
- 43% of companies that do have a business continuity plan do not test it annually.
- 50% of businesses experiencing a major computer outage will shut within five years.
- 90% of businesses suffering a major data loss from a disaster close within two years.

Source: London Chamber of Commerce

The nature of DR plans varies widely from one organisation to the next. For some it may be as simple as maintaining an off-site back-up. This can be okay providing, if disaster strikes, the physical business premises and hardware aren't affected, and providing the back-up captures up-to-the minute data that can be restored in minimal time. For other organisations the DR strategy involves a significant investment in secondary off-site data centres that mirror every action on the production machines. Duplicate hardware systems offer full redundancy, and alternate communications links provide the surety of continued phone and data connections. For most organisations however, the most appropriate strategy lies somewhere in between.

DR plans are typically determined by a few key considerations such as the nature of the business, the kind of data captured and the priorities for this data. Think about how downtime will impact customer service, contractual commitments, compliance, and the bottom line. What are the most essential technologies and systems if the business is to continue to operate? For example, in a transaction-based organisation such as an online retailer the loss of even fifteen minutes worth of data could be devastating whereas a small

engineering firm may find daily back-ups sufficient. Within a bank or financial institution continuous mirroring or duplication of data may be necessary.

By working through these kinds of questions, you'll be able to define your exact DR requirements including frequency of backup, hardware and communications needs, ideal restoration time and restoration priorities.

There's more to a business than IT systems

Although a DR plan offers some reassurance for IT, it is still a long way from being a complete business continuity (BC) strategy. Yet many businesses use the terms "disaster recovery" and "business continuity" interchangeably. The truth is that these are very different concepts and each contributes an essential role to ongoing business activity. Disaster recovery is a term widely used to refer to IT services – and usually only in relation to a "system failure" scenario, not covering situations when IT staff are unavailable or when IT staff aren't able to access the main building. Business continuity addresses the non-IT resources and non-IT related disaster scenarios, such as a major impact on the people, processes, physical facility, communications and suppliers.

There is little point having a DR plan if there's no office to work from or, as happened in the aftermath of the Christchurch earthquake, key staff are unavailable because they need to attend to crises within their own homes and families. This is a situation common to natural disaster areas. The flood, fire, cyclone or earthquake that has affected the business will also be taking its toll on your workforce. Public transport may no longer be available making it difficult to get to work and the roads may not be passable for private cars.

> Mobile telecommunication services are often considered a fall-back for organisations in time of disaster. However, during the 2011 floods in Queensland, telephone land lines and the mobile network were all out of action. Companies were faced with no means of communicating their predicament to staff, clients, partners or suppliers.

The role of the BC plan is to pick up where DR leaves off. BC looks beyond IT to provide a holistic view of all interactions and interdependencies both within and outside the company.

What you need to know about Business Continuity

The following ten points highlight some of the most essential considerations and inclusions for any Business Continuity plan (BCP).

1. Broadly speaking, there are **five key areas of impact in a disaster**: the building/office may not be usable, people may not be available, the IT system may be down, voice and data communications channels may be unavailable, and key suppliers may be out of action. Your plan will have to address at least these core effects.

2. BCP relies on a solid **plan activation and decision-making framework.** Take note of your organisation's critical skills and of the people who need to be authorised to take action in a crisis. Remember that some management and staff are likely to be unavailable so the framework needs to specify alternative decision makers and sources of approval across the company.

3. **Never entrust BCP to a single department**. Asking individual departments to create their own plans is the best way to ensure that departmental interdependencies fall between the cracks. What you need are multi-disciplinary, **multi-departmental BCP teams** and who can work together to assess, recover and resume time-critical services.

   For example, if disaster hits and the office can no longer accommodate all staff, you may need to consider equipping some people so that they can work from home. Facilities staff will need to find a way to support those already in the building. IT will need to get systems and communications to those at home and in the office. Marketing has to manage essential staff, client and other stakeholder communications. The BCP team needs to map out each activity and its impact on other areas of the business.

4. Communication is key. Create a streamlined **communication plan** that allows you to get news and information out to key players quickly. The best way to do this is by using multiple mechanisms in parallel. This could mean sending out messages via a secure staff blog, SMS, home phones, pagers and email all at the same time. The greater the number of channels, the greater the likelihood the message will get through. It is now possible to request and track acknowledgement by the recipient that the message has been understood. Prepare the plan well in advance of any disaster and communicate it to all relevant staff and management so that everyone knows what to expect and where they should be looking for information.

5. In case communications are completely unavailable or unreliable, make sure your BCP includes a suitable, pre-agreed meeting place or crisis control room so key decision makers don't rely on phone communication in order to get together and start developing a response strategy.

6. Focus the plan on core **impacts** rather than causes. If everyone is locked out of the building, does it matter whether it's because of a gas leak and explosion or a fire? In terms of business continuity, what you need to deal with is the effect of the lock-out. Develop contingency plans for all five key areas of impact (refer point 1) and anticipate that in a real disaster, you'll probably be dealing with a combination of these problems. How will you respond if a key supplier is out of action? If your telecommunications provider is down? If the building is no longer usable?

7. **Dual supplier** arrangements are a safer bet than appointing an exclusive supplier. It's best not to have all eggs in one basket when it comes to time-critical services.

8. When the BCP is ready, conduct **training and awareness** programs for BC team members as well as general staff. Define roles and make sure that everyone knows what they have to do throughout the three phases of a disaster – initial response, recovery and business resumption.

9. Conduct regular **tests, rehearsals and walk-throughs** with test teams of varying composition. It's important to find out that the plan works in a practice situation rather than under the stress of an actual disaster. Rehearsals also play an important role in hard-wiring processes into everyone's minds so that the right response becomes instinctive.

10. Adopt and provide staff with a good set of simple, up to date best-practice **BCP documentation templates.** Staff may not have time to hunt through a lengthy planning document to determine which steps need to be taken. Colour coded templates with bullet style information are a much handier reference and make it easy to update processes and keep staff informed. No business remains static from year-to-year, so regularly revisit the plan and update as necessary. The 'Business As Usual BCP framework' is a pre-populated set of templates that can save you months of work.

There are immediate financial benefits

Establishing DR and BC plans may be required for compliance, they may make an organisation feel better about itself and there are also benefits to reputation. If a large scale disaster hits your city and your organisation continues to operate, you're likely to gain a major advantage over competitors. Your company's ability to continue becomes a sign of reliability, good organisation and competence.

More importantly, there are also significant, immediate financial incentives for planning ahead. Companies that have a documented BC strategy can typically negotiate a discount of between 10 to 15% for their business interruption insurance premiums. It's an immediate

financial reward that provides a tenfold return on the effort of creating the plan in the first place. It's a persuasive argument when selling the need for BC to other senior management.

In addition, you may not be able to do business with Government or financial customers who are under strict BC regulatory requirements, which flow all the way through to their third party suppliers needing to have solid, tested BCPs. Without being able to show your BCP, you may not even be able to respond to a Request for Tender.

BC and DR strategies aren't rocket science but they do take time to create. To be effective they need to be thorough, well thought out and they must cover all critical bases. That's why it can be useful to seek expert advice from an external organisation that can help you to assess systems, recognise the critical processes within your operation, identify data and process interdependencies and step you through the priorities of recovery and restoration.

After all, the first time your plans are likely to be fully tested is in the event of an extraordinary disruption to business. And that's no time to discover a flaw in the strategy.

Professional Advantage works with companies who seek to improve the performance of their business through the application of technology. By focusing on solutions across all major organisational areas we help our clients to increase revenues and profits, control and reduce costs, improve efficiencies, achieve better value from information, better manage performance of overall business down to individuals and improve planning to achieve better returns on assets and resources. Our 250-strong team in 6 offices across Australia and internationally has successfully worked with over 1000 organisations including well-known companies such as AFL, Starbucks Coffee Australia, GHD, Department of the Arts, Sport & Recreation, Mundipharma, Hays Personnel, Muffin Break, Austar and many others.

Business As Usual is a BC specialist consultancy which assists organisations with BC Health Checks (pre-audit assessments), executive/board presentations, benchmarking exercises, Disaster Recovery rehearsals, BC training, marketing and awareness programs. It also assists with integration of BCP/DR and ITIL (IT Infrastructure Library, ITSCM) and HB221, BS2599, APRA and CobiT compliance.