

# Planning for survival

**Companies need to take action to ensure business continuity, writes Kevin Fitzgerald.**



**D**isaster recovery planning was the original label given to recovery planning when it first emerged in the early 1980s. It became critical in the 1990s as computer networks had been embedded within the fabric of most organisations and business decided it required something that recovered the business services not just IT. Thus emerged the business continuity plan (BCP) with a very definite business approach.

In the current decade the recovery plan requires further refinement. Interruptions now occur quite regularly as the IT infrastructure assumes a larger role in the provision of business service in many organisations. These interruptions are usually slight reductions in the service level, usually less than half-an-hour or so. They are not “disasters”, rather interruptions to full service that can be worked around in the main. The recovery planning reaction has been to develop emergency recovery procedures (ERPs).

So from DRPs to BCPs to ERPs we have come a long way but it is still not enough. Many organisations continue to ignore the need for effective recovery planning.

Changes in the approach to recovery planning over the last two decades came about because of the changing role of the computer. In the 1980s it was only computer management that recognised the need to provide protection against loss of IT services. This was fair enough because the computer environment was centralised around mainframes thus the responsibility belonged to the computer department. In 1985 if you could recover the computer services you more or less recovered the business.

However, the arrival of networked computing in the early 1990s reduced the importance of the mainframe. By the time every office had a desktop computer, the DRP, which focused on IT recovery only, needed to be reviewed. So the BCP arrived in the mid 1990s.

The BCP is much more business oriented. The standard approach involves six stages:

- i.** Business Impact Analysis – defines the maximum time period each business function can last without computing services before serious repercussions;
- ii.** Contingency Strategy – developed with each business function that allows the function to stretch its tolerance period by the development of business workarounds. It also develops stand-by facilities to match the final tolerance profile of each function. From this “hot” sites, “warm” sites and “cold” sites emerge. To match these designs off-site tape back-up cycles, power backup, communications rooms, and other essential elements of the infrastructure are also addressed;
- iii.** Site Toughening Exercise – this is conducted so that the potential for the loss of computing services is minimised;
- iv.** Detailed Recovery Plan is designed which forms recovery teams, establishes action deadlines, sequences, and responsibilities all aimed at recovery within the tolerances of each business function; and
- v.** A Test and Maintenance program is instigated so that the plan details are kept current, the technical capabilities are regularly proven, and the teams rehearse from time to time.

This BCP process is much more rigorous than the DRP process. The latter usually omits the business impact study, site toughening, tests and more often than not the detailed recovery plan itself.

DRPs and BCPs exist to provide cover for management when a major incident becomes public knowledge. ERPs address those short-term interruptions which do not or should not become public knowledge. ERPs consist of a set of standing orders detailing how to handle each likely interruption. Whenever an

**‘Many organisations continue to ignore the need for effective recovery planning.’**

unanticipated new incident occurs it will be added as a new ERP.

There has been much spoken about business continuity recently as an IT governance issue but very little action. In Australia, less than 15 per cent to 20 per cent of organisations have committed to a BCP based on the above six steps.

In frustration IT management are once more promoting the development of a DRP. They are implementing a recovery plan within their own resource and budget limits, which they know will not satisfy business recovery requirements. It is made abundantly clear that it is up to business management to fulfill their business recovery requirements from within their own resources and budgets. The service gap left by the DRP will be obvious. IT management has taken the lead and now it is up to business management to complete it. If the business wants to achieve an acceptable recovery it will need to design the BCP around the DRP already put on the table by IT management.

This strategy may at last help prompt some much needed action in this area of information security before someone goes to jail for failing to fulfill their duties as a director. □

**KEVIN FITZGERALD**  
 is an information security consultant with more than 25 years experience in designing and executing security solutions for large organisations.