

BCP: It's time to get serious

Kevin Fitzgerald says business continuity planning is vital in the uncertain times we live in.



The world has changed over the last few years, and both individuals and organisations are on a much higher level of alert to danger. 'She'll be right, mate' doesn't work anymore.

Management is conceding it must have some protection against disaster and corporate governance demands it. Accepted security standards are putting it in black and white: organisations require a business continuity plan.

A BCP typically consists of the following six phases.

Phase 1. Business impact analysis

Based on a variety of impact scenarios, this determines: critical tolerance periods the business can withstand before its ability to recover is threatened; the order of business process recovery; and the costs, both tangible and intangible, that will result following a significant interruption based on the current

level of preparedness.

In this phase, management must understand the criticality of the BCP project, the need for a long-term commitment, and that 'over-engineering' of the solution can be avoided by understanding the recovery needs of the core business applications. The estimated costs of a disruption will provide motivation to reduce the likelihood of disruption to be explored in Phase 2. The process priorities will lead to contingency strategies that will reduce the effect of interruption, which are designed in Phase 3.

Phase 2. Business function toughening

A physical and logical review of the business processes is conducted so obvious weaknesses can be controlled immediately within priority needs, budget and business case constraints.

Management receives a 'quick fix', and a plan for

future fixes should there be others identified but not attended to because of budget constraints.

Phase 3. Business contingency strategies

This phase develops supporting infrastructure to maintain critical business processes through the four typical stages an organisation goes through after a significant disruption: emergency, workarounds, recovery, and recuperation.

The contingency strategies report includes solutions encompassing damage minimisation, staff retention programs, customer retention programs, public relations control, business process workarounds, mail, telephone, fax, and email communication services, backup data recovery, contingency equipment and facilities, staff work programs and processes for each post-disruption stage. As part of this phase, an overview of the whole recovery project, a 'recovery roadmap', will be provided to guide Phase 4.

Phase 4. Detailed continuity plan

A continuity project plan should be devised around a management team who will work closely with the command centre team to coordinate tasks within the tolerance period defined in the business impact analysis in Phase 1. The four stages of post-disruption experience will be covered. Time and task targets will be monitored by the command centre throughout the process. A detailed project plan is developed with the input of key players to allow continuity of the business. The plan will be accompanied by a database of essential information, including an inventory of all assets, insurance details, contact lists of all executives, key staff, emergency services, and participants in each stage

'Over-engineering a recovery plan will lead to management opposition. Common sense is required.'

of the recovery process. The initial plan will require fine-tuning and this will occur through regular review, testing, and exercising of the plan.

Phase 5. Test and maintenance

A series of tests will be designed, focusing on the ability to achieve the objectives of a particular task, series of tasks, a business unit, or the enterprise as a whole. What happens 'in the first five minutes' can often determine the success or not of the recovery.

Test objectives and critical success criteria will be established and used as parameters to judge the success of each test. Changes in the recovery database will occur over time, including contact numbers for participants, asset details, and supporting resource requirements. Time tolerances may also change as the nature of the business changes. Recovery plans must be kept current with regular test and maintenance schedules. However, once again over-engineering such a schedule will lead to management opposition. Common sense is required.

Phase 6. External audit

An independent review of the implemented plan is of course mandatory. □

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