

# Making a case for continuity

**It's high time businesses fastened their seatbelts, writes Kevin Fitzgerald.**



In a way, BCPs (business continuity plans) are similar to seatbelts in a car. Before they existed and before they were compulsory we just accepted that injuries and deaths in cars were an unavoidable potential consequence of owning a motor car.

Now that seatbelts are fully accepted (and compulsory), they have become part of the driving experience — for most people, at least. We feel safer because of them and those who shun them are considered foolhardy when the evidence so strongly supports their use. And when we go to countries that do not enforce seatbelts, and sit in the back of a taxi untethered, we feel decidedly unsafe.

Taking the seatbelt experience and comparing it to the use of BCPs in business, what do we find? Because less than half of Australian businesses have ever conducted a BCP project and, of those, perhaps only half have regularly maintained their plans to keep the

information current, only about 25 percent of Australian businesses have a BCP they can trust — as if only 25 percent of cars had a reliable seatbelt! And these figures are conservative. Others have claimed that less than 10 percent of businesses have plans that would be effective in countering a significant interruption.

However, it could be argued that there is no comparison between the effectiveness of a seatbelt and the effectiveness of a BCP. It is true that it takes commitment to ensure that the BCP is regularly tested and maintained. It is also true that the BCP should not be over-engineered; it should be kept as simple as possible, because the more complicated it is the more difficult it is to keep it current.

One way to keep the BCP simple is to ensure that it is designed to recover the business within its maximum acceptable outage period. In other words, can the business tolerate an interruption to its business

outputs for, say, 10 weeks, 10 days, 10 hours, 10 minutes, or 10 seconds?

It is very important that a realistic assessment of this tolerance is made. It is rare that a business would require a 10-second recovery. However, companies based on online technologies may well require this tolerance for some business functions. Few businesses will need the BCP to recover the business outputs within 10 minutes. More will comfortably fit within the 10 hours to 10 days (perhaps 20 days) category, but not many will accept delays for longer than this.

Businesses may also argue that the risk exposure for a driver in a motor vehicle is far greater than the risk of a business suffering from a significant interruption to its business outputs. Nevertheless, we all know that businesses suffer from fires, floods, power outages, air-conditioning breakdowns, lift breakdowns, union actions, political protests, transport problems, burglaries, theft of equipment by staff, loss of key personnel, and many others.

It is very easy to say: 'We haven't had a problem for 50 years. Why worry now?' However, whatever the odds, and it is gambling when this argument is used, it may still happen. It is the responsibility of the directors of public companies and government departments to assure their shareholders and taxpayers that they have the plans in place to enable business continuity.

So what does it cost to build, test and maintain a BCP? Part of the 'build' component is the investment that must be made in contingency facilities or services. The lower the maximum acceptable outage period, the more expensive the stand-by solution. Insurance premiums may be used to offset these costs. Virtual rather than bricks-and-mortar stand-by will also help.

**'Only about 25 percent of Australian businesses have a business continuity plan they can trust.'**

The ranges shown in rough estimates below are attempts to accommodate the ranges of tolerance and stand-by options available in the marketplace.

For a large organisation, it will cost around \$70K-\$100K to establish a BCP, \$20K-\$30K a year to test and another \$20K-\$30K a year to maintain. For a medium organisation, it will cost around \$40K-\$60K to establish the BCP, \$15K-\$20K a year to test, and \$15K-\$20K a year to maintain. For a small organisation, it will cost \$20K-\$25K to establish, and \$5K a year each to test and maintain.

Against these cost estimates is the safety of the organisation provided by a BCP that is kept current and effective. An organisation with a BCP has the opportunity to survive a major interruption without significantly jeopardising its customer base, its people assets, or its information assets. Equipment, fixtures, fittings and accommodation can all be replaced, but the loss of customers, management, staff and information may well result in the organisation floundering and eventually dying.

Like a seatbelt, a BCP provides safety in times of trouble. Just because it doesn't happen every day doesn't mean that it can be forgotten. It is its own type of insurance. □

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