Print Close

Librarians rewrite the book on disaster recovery

Nate Cochrane | Jan 18, 2011 7:08 PM

But four-fifths of Australia's IT workers are not so confident they could reboot after catastrophe.

Print Close

When flood waters threatened to breach the banks of the Brisbane River last Wednesday, the State Library of Queensland looked to be one of its first casualties.

Fortunately for the library and Queensland's bookworms, management had a well-developed disaster recovery plan that went beyond simple data backup and that included all the minutiae of surviving catastrophe so that librarians didn't have to make it up as they went along.

As the water started flowing into the basement levels, the library's client services director Rory McLeod and staff swung into action.

"It was about following basic disaster procedures," McLeod said.

"Once we knew water encroached into the basements we knew there was a chance that we would lose power so it was about getting [backup power] checked and online and taking down essential systems as quickly as we could."

The library systems were replicated and a library principle is "lots of copies keeps stuff safe - so it's quite easy for us to point people at different servers at other state libraries", he said. The collections were safe and systems were being brought back online as staff returned.

McLeod's confidence in being able to recover in the face of disaster was reinforced by a written and annually updated disaster plan that included what to do to physically secure and protect an installation and how to handle the inevitable staff absences at a time of great stress. It included disaster scenario planning procedures to cater for contingencies.

McLeod, who was also evacuated from his home, said mobile devices presented a new crimp because so much information was stored online or people could not be contacted when there was no landline alternative.

McLeod said the best approach was to keep multiple copies of documents in various locations and to keep redundant providers and networks so that in times of near-total devastation there were alternatives paths. Another lesson was to keep redundant lines of communication: "We found that when one provider was down, another was up", allowing workers to stay in touch with each other and their families, he said.

"Our recovery plan was put to the test for the whole organisation and [our] complexity means we have to keep everything from normal IT systems to digital library systems

that may retain original materials such as ebooks where there may be only a few copies," McLeod said.

He was confident that as staff came back to work and systems were rebooted that the library network would survive: "Everything so far that we're bringing online has been coming back OK".

Librarians have long planned for disaster, the Australian Library and Information Association reminding members this week that the floods were "a timely reminder to dust off your disaster plan for the year ahead, in the hope that you may not need it".

That was in part a response to the Brisbane floods that threatened the state's holdings and that damaged stock at libraries such as Laidley in the Lockyer Valley, about 60 kilometres west of Brisbane. The group also conducted a study in the aftermath of the 2009 Victorian bushfires that led to improvements in how to handle disaster.

Library association executive director Sue Hutley said even model organisations would suffer with such total devastation.

"Even the best-funded organisations may not have been able to meet the challenges of IT backup unless they had an interstate server," Hutley said. "Smaller organisations tend to have backup servers in the same state."

In Brisbane, several data centres were knocked out of action during the floods, often due to optical-fibre network breaks.

Hutley said rising floodwaters took down the Queensland State Library website for a few days, but the shared Trove online database meant borrowers and staff still had access to collections, telecommunications permitting.

The association website provided templates and case studies to help libraries plan for disaster and member libraries will meet next month in Queensland and Victoria to share what they learned from the recent inundation.

"Online backup services will give libraries another point to consider," she said.

Confidence drained

But not all organisations were as confident in their abilities to come back from the brink, a report released today found. It showed that boardrooms were denying Australia's IT departments the backing they needed to recover swiftly in the event of a disaster.

The confidence index of 3000 IT workers by the US Ponemon Institute commissioned by backup and storage software maker Acronis found Australian small to medium-sized businesses were near the bottom of an international league table when it came to director support of disaster recovery systems.

Despite spending around the middle of the heap of the 13 countries surveyed, Australian IT workers and said lack of board support sapped them of confidence their organisations could weather disaster.

It found the 259 IT workers surveyed from Australia were the least confident: nearly four-fifths doubted their ability to recover quickly compared to the average 50 percent and the global leader, Germany, at about a quarter of respondents. Just 14 percent of those surveyed were directors or executives - the bulk were technicians (30 percent), IT managers (17 percent) and supervisors (14 percent).

"Support from the boardroom, which is where IT budgets are won and lost, is evidently a foundational requirement for IT managers to have confidence in their backup and [disaster recovery] operations," the report's authors wrote. "The study also shows that businesses with the highest executive-level support also suffer the least in terms of downtime in the event of a serious incident."

Acronis country manager Simon Howe said the report did not measure capability.

"The intention is an IT user can look at this and see what is giving my peers confidence and how to incorporate best practice into their environments," Howe said.

He said that business leaders tended to place disaster recovery low on their priority list, although many of those surveyed in Australia would have been business owners who had to weigh the risk of losing their business data against the cost, he acknowledged.

Speaking up

But the managing director of Sydney IT security and assurance consultancy Securus Global, Drazen Drazic, was sceptical of the report's findings. He said a board properly informed would act on serious matters.

"In cases where people feel they haven't the support, was there just an assumption that the board was not backing them when in reality, was the board even aware of their concerns?" Drazic said.

"Did the appropriate message get conveyed so an educated decision can be made? Backup and disaster recovery is more ingrained than other security issues where you expect lower figures."

Drazic said that when IT thought it wasn't heard, it may be because it wasn't high enough up the pecking order or the organisation was bifurcated, separating IT from the line of business.

About a third of Australian organisations surveyed didn't have an offsite backup strategy: "These countries were generally the most likely to claim backup and [disaster recovery] was not being made enough of a priority, citing lack of budget and resources," the report said.

The lack of acknowledgement in Australia's boardrooms didn't affect spending greatly: although Australian organisations spent on average 11 percent of their budgets on disaster recovery, less than the global leaders Germany and the Netherlands, it was not by much. And average spending among those most confident varied from 6 percent in some Asian countries to 14 percent in parts of Europe.

IT managers running operations in financial centres Switzerland and Hong Kong were among the most confident they had the ear of directors and could get back up and running swiftly after catastrophe.

Cloud

The malaise in Australian organisations' ability to reboot operations seemed to come from poor controls and policies - more than half of Australian IT managers responding they had none compared to just 15 percent in those organisations operating in leading countries. In the US, 60 percent of respondents said they had written documentation to follow in the event of failure.

This absence of structure flowed through from physical backup to virtual servers, the report's authors finding nearly half of Australian managers backing up their cloud storage less often than their physical servers: "The fact that they treat virtual and physical backups differently can probably be attributed to a lack of resources and technologies".

About a fifth of Australians surveyed said they would spin up cloud services in the next year compared to 16 percent who had them last year, in keeping with the global trend. But cloud was still the less-travelled route, most organisations replicating offsite over virtual private networks.

The biggest hurdles spruikers of cloud services faced were perceptions recovery from the cloud was slower than existing alternatives, suffered poor security, and were unnecessarily complex.

"Businesses will continue to perform local backups and recoveries for speed and use the cloud for an additional layer of protection, long-term retention (replacing tape) and site failure," the report said.

Half of Australian organisations saw the cloud as a way to lower costs while a fifth - among the highest response in the survey - preferred it over alternatives for its quality of infrastructure.

Howe said that Australian small businesses were well aware of the benefits of backing up to the cloud but struggled with multiple backup solutions for different platforms, such as to devices in their premises, offsite and in the cloud with up to a third using five solutions.

Acronis was contacting its customers in flooded areas to offer support and advice to get them back on their feet quickly, Howe said.

The survey conducted last October and November asked 3000 small to medium-sized business respondents in 13 countries to show their agreement to questions such as "We have ample resources that enable comprehensive backup and disaster recovery" and "We would not suffer substantial downtime in the event our organisation experienced serious incident or event". Small to medium-sized was defined as up to 500 seats in Australia and up to 1000 seats elsewhere.

Donate to help the flood survivors in Queensland and Victoria.