BRENNAN IT

DISASTER RECOVERY

Ensure your business technology is there when you need it

By Lyncoln De Mello, Director - Cloud Services

DISASTER RECOVERY: ENSURE YOUR BUSINESS TECHNOLOGY IS THERE WHEN YOU NEED IT

When it comes to natural disasters, Australia is relatively safe from the devastating tornadoes, volcanoes, and earthquakes that haunt businesses operating in many other countries. But businesses in this country still face many potential disruptors – including floods, bushfires, power failures and telecommunications outages – and each of these has the ability to bring down a business for hours or days at a time.

The costs of such events can be extraordinary, recent reports by the Australian Business Roundtable for Disaster Resilience and Safer Communities predicted that the social cost of natural disasters to Australia will grow from $9 billion to $33 billion per year by 2050. In addition, by that time natural disasters will have required the construction of $17 billion worth of critical infrastructure.

Those forecasts are at least 50% greater than had been previously estimated – highlighting the growing cost of disasters to Australia. Yet for individual businesses, the potential costs of business interruption can be even more significant, with losses from business and supply-chain interruption easily reaching the millions and long-term interruptions potentially pushing companies out of business.

Disasters don't only affect companies' IT organisations – but if they do, the entire business may stop operating until they are resolved. When Qbot malware recently took down the network of major healthcare operation Melbourne Health, staff in catering, pathology and other areas were forced to adopt manual procedures and workloads were slashed so that only urgent samples were processed.

As many businesses learn the hard way every day, they are often only one technology fault away from disaster. IT planning is therefore critical to businesses of every size – and this includes the need to build Disaster Recovery (DR) plans to be ready should the unexpected happen. However, surveys across a wide range of industry segments repeatedly suggest that DR planning is still far from front-of-mind in many businesses.

> Data loss and downtime has cost Australian organisations around $65.5 billion (US$55 billion) in 2014, according to research conducted by Vanson Bourne. Almost two-thirds (64 per cent) of the 125 Australian companies surveyed experienced data loss or downtime over the period.

> The average organisation experienced more than three working days (27 hours) of unexpected downtime. Other commercial consequences of disruptions were loss of employee productivity (54 per cent), and loss of revenue (44 per cent), the survey found.

The majority (78 per cent) of Australian organisations are still not fully confident in their ability to recover after a disruption, and companies with three or more vendors lost 10 times as much data as those with a single vendor strategy, the research said.

Another piece of research in late-2015, a survey by Kroll Ontrack, which specialises in recovering data from damaged hard drives and other storage media, found that two-thirds of companies don't regularly test their DR plans. Of those that do, just 9 percent of companies tested their DR plan every 1 to 5 months, and 29% tested their plan every 6 to 12 months.

Another, earlier Kroll Ontrack survey suggested that only half of Australians had backup solutions in place – well behind the 65% figure recorded across North America, Europe and the rest of the Asia-Pacific region. Of those, 64% said they had lost business data in the past. Asked why they weren't more fastidious about backing up, 49% said it took too much time to do properly.

These results – and those of another recent survey by US insurance firm Nationwide in which 75% of small businesses said they don't have a DR plan in place and 38% said such a plan wasn't important – raise very real concerns for the protection of businesses should unforeseen events cause major problems.

Effective DR planning must lay down comprehensive plans for maintaining key business processes in the event of an IT systems failure or communications interruption. And, because IT is continually evolving, it's essential that plans are regularly tested and revisited to accommodate new technological developments that either change the systems used by the business, or offer new methods for improving its DR response.

BUILDING A DISASTER RECOVERY PLAN

Just what elements go into a DR plan change depending on who you talk to, but all will address key concepts such as redundancy and business continuity.

Recent advances in IT have made redundancy an easier and more cost-effective capability: building redundant systems used to require companies to buy multiple, expensive servers and to maintain expensive secondary failover data centres. For example, the spread of server virtualisation has obviated the requirement for duplicate server hardware.

Use of virtualised servers allows businesses to easily shift key servers between sites, whether for adding additional capacity or for maintaining operations in the event of a primary systems failure. A proliferation of hosting providers offer high-speed, highly scalable platforms on which companies of all sizes can build DR environments; in the event of a disaster at the main business premises, key systems can be redirected to the hosted environment and the business can resume operations as quickly as possible.

> Modern cloud platforms take this a step further: in many cases, businesses are migrating key systems to the cloud with the knowledge that those systems will be available even if critical infrastructure affects their primary site.

These platforms offer enough scalability and internal redundancy that they can offer a level of reliability – even for small, resource-constrained companies – that was unthinkable a decade ago. A great example is ASX-listed toymaker Funtastic, who have leveraged a cloud-based DR solution, which replicated data from numerous mission-critical virtualised servers into the Brennan IT's infrastructure in real time.

> “If we have a disaster here and are down for a day that's going to cost us $35,000 in just salaries, rent and utilities,'' Mr Bennett said. “That's $4500 per hour for staff and about $70,000-odd if you include lost sales per hour. With what we are using now, I can just log into the portal or Brennan IT can on their side — click a few buttons from the main screen and do failover.”

As well as technical considerations, business continuity also requires a raft of organisational planning that should be conducted in concert with technological measures. Key business functions, for example, need to be elucidated and stock taken of the staff needed to deliver them. Backup premises will also need to be identified, offering enough desk space to host staff on spare laptop or desktop computers for the duration of the interruption.

It's important to remember that complex supply chains, of the sort that businesses rely on every day, require the ongoing coordination of business processes with many companies at once. Even where the end customer is not affected, a disaster may affect one or more suppliers down the supply chain – causing logistical issues that interrupt the otherwise-intact business. For this reason, effective DR planning also requires working with suppliers and partners to ensure that they also have effective and current DR plans in place – and that those plans include your business.

Just as each company's business is unique, so too will its DR plan be unique. For this reason, a crucial element of any DR plan is documentation. From the earliest stages of the DR plan, it's essential to carefully and methodically document the IT infrastructure, key applications and the hardware they run on, information about related support contracts and technical contacts, and so on. Modern applications have extensive interdependencies and these must be discovered and documented to facilitate root-cause analysis in the event of a systems failure.

Documentation must also include detailed information about server and application configurations, as well as information such as the location of backups and the details of hosting or cloud providers running the applications. It must also be readily available – ideally in paper form or hosted offsite to ensure it remains available even in the event of a total systems failure – and multiple key staff kept apprised of how and where to find it.

WHEN IN DOUBT: TEST

Disaster recovery plans tend to expand and change as the business and its supporting infrastructure grow over time. The key to keeping it fresh is to consider your entire IT and business environment as a tightly linked, functional whole – and to consider enlisting the help of outside DR and business continuity professionals who have been there and done that.

For example, at Brennan IT we can help you inventory your crucial data and applications, then develop a robust backup plan that ranges from simple tape backup to full-time cloud replication. They can help formalise the processes involved in moving your staff and resuming your business from a secondary site. And they can help review your existing IT and communications infrastructure to evaluate your current DR processes as well as recommending areas for change.

Indeed, there are so many facets to a DR plan that one very real decision every organisation faces is just when to stop. Creating a mirror of your entire IT infrastructure may be possible, but it is likely to be extremely expensive and may overcomplicate your DR execution by masking your core business priorities.

In working through your DR assessment, it will be valuable to prioritise each business function and its likely impact – whether tangible, intangible, direct or indirect – should it be interrupted. Map internal dependencies and consider alternative suppliers or staff that can be brought into the picture if necessary.

Most importantly, as any DR specialist will tell you, when it comes to ensuring business continuity it cannot be overstated how important it is to test, test, test. After all, the seemingly best-laid DR plan is worthless if it is never put through its paces in a real-world scenario.

At the basic level, this includes running 'tabletop' simulations with all key players in a room and an organiser who describes the scenario playing out in real time, and adds occasional surprises to test staff flexibility. As a completely theoretical exercise, tabletop testing also allows collaborative evaluation and refinement of plans as well as the positing of what-if scenarios that may result in changes to the DR plan.

Functional testing offers the chance to test actual procedures and policies by drawing actual IT staff into the game. A business-continuity team leader might tell key staff that a branch office had gone offline and see how long it takes them to recover operations at that site, or they might test data-recovery procedures by instructing staff to restore copies of one or more databases from cloud-based backup service. This testing puts DR plans in real-world context by exposing communications gaps or areas where technology can be streamlined.

Any disaster recovery professional will tell you that protecting your business is much more than a one-off exercise; it's a state of mind that must extend across every level of IT and business operations. By planning ahead and working together, it's possible to develop and maintain a highly effective DR plan that will guide your response in times of adversity – and ensure that you're back.

Are you ready for the unexpected?

In the event of a fire, flood, or even virtual disaster such as a network failure, can your business recover quickly, stay online, and service customers? Click the link below and take our quick quiz to see how ready you are for the unexpected?

www.brennanit.com.au/ready-for-the-unexpected

References

1. The Economic Cost of The Social Impact of Natural Disasters, http://australianbusinessrountable.com.au/our-papers/social-costs-report

2. Building Resilient Infrastructure, http://australianbusinessroundtable.com.au/our-papers/resilient-infrastructure-report

3. Royal Melbourne Hospital attacked by damanging computer virus, http://www.theage.com.au/victoria/royal-melbourne-hospital-attacked-by-damaging-computer-virus-20160118-gm8m3v.html

4. Most Small Business Onwers at Risk for a Disaster, https://www.nationwide.com/about-us/083115-small-biz-survey.jsp