

Disaster recovery produces testing tales

By Siobhan Chapman, ComputerWorld

11 April, 2002 15:57 Sydney, Australia

Data centre managers and analysts say that disaster recovery testing has bloomed since September 11. Yet, according to tales told to Computerworld of shortcuts taken in disaster recovery testing, or elements overlooked in processes, the door could still be ajar to disasters.

A systems administrator for a national telecommunications company said the company recently ran a major disaster simulation as part of IT testing. Although it was a simulation of a full-scale disaster, the telco did not evacuate its telephone exchanges.

The systems administrator, who requested anonymity, said that, in the case of any threat to a company's assets, an exchange, with its full complement of staff, would be the first target.

This is just one tale of disaster recovery short cuts which should serve as a warning to IT professionals.

Terence Giufre-Sweetser, IT consultant at wholesale ISP services company TereDonn Telecommunications has more "tales of woe and begone".

"How about an unnamed government department who never tested their backup tapes and found them useless upon attempting to restore a dead file server? Or the two-hour replacement contract that couldn't. The part to be replaced was obsolete and the manufacturer was unable to supply a reconditioned unit for six weeks?" he said.

"Then there are the cheap clients who would not use off-site tape storage and retrieval. The place of business burns down. All records are lost. It killed the company stone cold dead," he said.

"We have no less than four Uninterruptible Power Supplies (UPS) here, for the servers, routers and even the PABX. The first real 'disaster' is the conversion board in the big UPS dies, resulting in no power to the servers," Giufre-Sweetser said.

David Solsky, director of sales and marketing at storage provider, SecureData Group, had more anecdotes of witnessed disasters.

"I've seen companies take four days to recover. Eight to nine hours to get the data up from tape, and then the remaining three and a half days was because of an inability to get the proper hardware. This should all be proceduralised," Solsky said. "One of the worst-case scenarios I've witnessed is a client that couldn't recover because backup tapes failed or corrupted and they had never done tests to restore from tape."

Awareness of the importance of disaster recovery has risen significantly since the terrorist attacks on the World Trade Centre. However, Simon Franklin, head of business continuity at Deloitte Touche Tohmatsu, said local IT is taking shortcuts in disaster recovery testing, and not getting the support from the business they need.

Franklin, who witnessed and assisted companies struck by IRA terrorist activities in Manchester in the UK, spoke to Computerworld about some of the errors in common disaster recovery policy committed by IT teams in the UK.

According to Franklin, many IT teams do not involve users in regular bi-annual disaster recovery testing, to the detriment of the test.

"IT shouldn't do these test alone, but should have involvement of users and customers. A number of times we have come across tests where just IT is involved, but the business users are not involved. Techies have brought the systems up and finished the test, but without the user. Therefore, they haven't met the objectives of the test and haven't debriefed on what, if anything, went wrong," Franklin said.

Complacency

Independent IT consultant Andrew Hennell, points out that IT needs to be aligned with the business. As a volunteer at the Australian Emergency Services Volunteers Network, Hennell has plenty of real-life fireside tales. He advocates business-wide disaster recovery planning, not just IT.

"My experience with disaster recovery plans is that they're insular within the organisation -- that is, the IT department will create its own plans separate to other areas of the business. Any good disaster recovery plan must be inclusive of all areas within an organisation.

"Most disaster recovery plans fail in that they look at the small picture. Often people don't look at single points of failure. For example, they may have four UPSes and a generator, but how much fuel have they got in the generator? Fuel goes stale within three to six months. Complacency kicks in very fast after a disaster recovery plan is put in place.

"While the IT world looks at specific disaster recovery plans, my work involves looking at that bigger picture, making sure that there's something for that IT department to do when it's back online as per its disaster recovery plan."