

# Planning for IT disaster recovery

As youngsters, we were all encouraged to eat our greens. If we did, or so we were told, we would grow up to be fit and healthy. The unspoken corollary was, of course, that if we did not, we would suffer from scurvy or be sickly like that little girl at number 43. It was our first lesson in prevention being better than cure. It is a lesson of which we should remind ourselves when thinking about disaster recovery.

*Nick Simms*

Most sensible managers, particularly those in the City of London, have given some thought to protecting their business against disruption. They may have signed a contract with a recovery service provider, possibly even created some sort of written plan. The really conscientious will have had someone in to look at the potential impact of interruption on their day-to-day operations. What many of them will have failed to do is learn from the pain of "eating their greens".

Research by International Data Corporation shows that terrorist acts, floods, fires and malicious attacks command over 80% of the attention of those preparing plans to combat disruption. Yet, over 80% of the incidents supported by third party recovery suppliers can be put down to altogether more mundane events — computer malfunction, power failures, virus infections and human errors.

Many in-house IT teams also spend considerable time recovering data that has been inadvertently wiped by users. In other words, most people who get as far as thinking about disruption spend their time planning for disasters they may never experience in their business lifetime, rather than for events they certainly will — possibly on a weekly or daily basis.

Major incidents, such as explosions or the proverbial plane dropping out of the sky, clearly present a real threat to the survival of any organisation affected, but so, often, do less obvious disasters. One stockbroker was closed down by the regulators following the loss of critical customer data. Another had to delay making a take-over bid on behalf of a client because of a power failure, with potentially very serious consequences for both it and its client.

There are a wide variety of measures that can be taken to minimise the likelihood of disruption. However, rather than rush in and install, say, a

back-up generator to reduce the risk of being without power, managers with responsibilities for computer and network systems should adopt a more systematic approach.

## **Business Impact Review and Risk Assessment**

The first stage is to win the backing of senior management for a Business Continuity programme. Without it, you will be doing the equivalent of trying to push a rock uphill; you will have no additional budget — so anything you do spend will have to come out of your existing resources — and you will struggle to get the business co-operating for the next stage of the process, a Business Impact Review.

This involves analysing the impact of disruption on each and every function of the business and its dependencies and working out the direct costs of disruption (for example, loss of sales), the potential and indirect consequences of disruption (for example increased insurance premiums in the future), the speed with which disruption will make itself felt and what impact the timing of disruption might have. This last point is frequently overlooked. Business priorities may be different at different times of the year/month/week, etc. A toy manufacturer, for instance, may emphasise product distribution in the run up to Christmas but payment collection in the weeks after.

Clearly, to do this exercise successfully, you will need the help of line managers, who are unlikely to contribute unless their bosses have already sanctioned the idea. Hence the need for senior management sponsorship from the start. It may also be easier to use a scale such as high/medium/low rather than trying to quantify potential losses down to the last pound.

# Planning for IT disaster recovery

Following the Business Impact Review, the next stage is a Risk Assessment. Here one looks at potential threats to business functions. Again, a scale can be used to measure vulnerability.

## Countermeasures

By combining the results of these two stages, a list of priorities emerges. The process of identifying and implementing cost-effective countermeasures can then begin. For, say, a key office process dependent on a server-based network, some PCs and a high-speed printer, the actions could include any or all of the following:

- taking regular copies of data and moving them off-site to reduce the risk of data loss
- adding more robust disk technology such as RAID (Redundant Array of Inexpensive Disks) to reduce the risk of disk failure (the most common cause of hardware malfunction)
- installing virus checkers on each of the systems, and perhaps removing floppy drives on the PCs, to guard against infections
- using lock-down devices and installing alarms to prevent theft
- installing back-up generators and Uninterruptible Power Supplies (UPS) to reduce the risk of power failure, and
- damage from fluctuating current and improved staff training to lower the risk of human error.

Insurance, maintenance and disaster recovery contracts should also be considered. A new option worth exploring is automatic electronic back-up of servers and PCs to off-site storage depots. This has the three advantages of ensuring critical data is stored off-site; reducing the risk of human error or laziness and allowing users to restore inadvertently deleted files without the need for intervention by the IT department.

Any measures adopted should make financial sense. Often organisations don't spend enough protecting the continuity of their business. Almost as frequently they spend a fortune protecting themselves against unlikely events that would not cost them very much if they occurred or on solu-

tions that won't work in an emergency because a critical dependency has been forgotten.

One famous example is the subsidiary of a major bank which invoked its disaster recovery contract following the bombing of the City of London only to discover that while it could restore its £10 million mainframe system, it couldn't restore a critical link to the United States which depended on a PC with a modem card costing a total of £1500. Luckily on this occasion, a technician who just happened to be visiting the recovery site on the day was able to hack into the bank's network and restore the link. Clearly, if security had been up to scratch, he wouldn't have been able to get in and the organisation might now be out of business.

A second example is the fire at an electrical sub-station in Lower Manhattan which cut off mains power to most of the banks in Wall Street for several days. In-house back-up generators kicked into action but within a day or two most had failed. Those that had been tested prior to the fire were typically tested for an hour or two every weekend — but not for an extended period. Many were also too small for the function they were required to perform, not having been upgraded for many years.

This example highlights why Business Continuity planning must not stop at the implementation of countermeasures. *Realistic* testing and updating is vital. Just like painting the Forth Bridge, Business Continuity should be seen as on-going task, not a one-off project. Assumptions relating to the Business Impact Review and the Risk Assessment need revisiting as the business changes.

Moving the focus from recovery to continuity ties in with today's emphasis on improving customer service. The first consequence of this is that continuity comes to be seen as a business-wide activity, not just something for IT management to worry about. Secondly, continuity can be shown to provide real business advantage and, therefore, is no longer looked upon purely as a cost — but as a benefit.