

## **Disasters: Recovery or Continuity?**

Not only has the increased risk of terrorism focussed people's minds on how their business would cope, but the recent series of natural disasters has shown how everyone is exposed to similar risks. Many organisations are now dusting off their disaster recovery (DR) plans and updating them to make sure they know what they would do.

A traditional DR plan looks at recreating the business in the event of total loss of the office, and can be scaled back for smaller problems, but there are now a much larger number of scenarios. Exclusion zones set up around actual or expected terrorist attacks may remove access to a building for one or many days, without actually destroying anything. Other disasters may be outside the control of the business; a major power or communications failure will be just as crippling as a physical disaster.

IT only forms part of the business that needs to plan for such an event, but carefully designed systems can make a significant difference. From the IT perspective, the issue is not disaster recovery, but business continuity; keeping things running regardless of what else happens. That is not to say that IT departments do not need to have recovery plans. Far from it in fact: all IT departments should have tested plans in place for recovering each server and system in the event of a failure, as a localised disaster such as a total server failure is in fact a likely possibility.

The key to good design of IT systems is to build resilience into the system that covers both failure of individual components and also loss of an entire locality. Once, this required systems and communications links that were beyond the reach of most organisations, but now such features are standard in many products and the cost of connectivity has fallen considerably. The other half of this design is that systems can be accessed from multiple locations, and ideally from any location including home. In this way any disaster that means people cannot work in the office is not an IT disaster, as they can carry on from anywhere they can find somewhere to base themselves.

Even where individual systems cannot be split over multiple locations (and much line of business software is still lagging behind in supporting this type of approach), the IT infrastructure as a whole can be spread. If key systems are spread over three locations, then it is unlikely you would ever have to recover more than a third of them as a result of any disaster, and what is more that recovery is likely to have access to a working network to link to. Many firms can take advantage of what has previously been an IT hindrance, namely that they have multiple offices, and either spread their core systems or place backup systems in other locations. Another option is to use a third party data centre to host systems, either with or without additional support services. Axxia provide this type of service to a number of their clients already. A data centre is likely to provide a much better environment for IT systems

that should increase the reliability of those systems as well as reducing the risks to the firm. An additional advantage is the wide availability of communications links at such a location, which can reduce costs as well as give options if one supplier experiences problems. In some cases, the cost savings in telephone links and internet connectivity can actually cover the costs of renting space in the data centre in the first place.

A final part of the puzzle is getting the backups right. Most organisations will be doing tape backups following some form of best practice, but also will know that this is a hard way to recover systems. It is now possible to back up to disk across locations, either to another office or data centre used by the firm, or by using a managed backup service. Either method gives much greater control of the backup, and importantly allows a much better recovery process as recovery can be prioritised down the individual file level if required. At the other end of the scale, full server replicas can also be backed up that allow a replacement or standby server to be recovered very quickly to an operational state.

To build a resilient IT infrastructure, there are really just three simple things to bear in mind, but they need to be thought about at the start as part of the low level design.

- Spread the risk; run systems from multiple locations
- Remove the dependency on location; design systems that can be used from anywhere
- Spread systems out; create systems that will run from more than location

From an IT point of view, disaster recovery is all about planning for business continuity. Done well, an IT department can not only save their firm a lot of money in the event of a disaster, but they could actually save the business.

*Adam Westbrooke is the managing director of Firstcourt, a strategic IT solutions company specialising in helping professional services firms. For more information call Adam on 0870 350 3660 or see <http://www.firstcourt.co.uk>.*