



# Taming the business of disaster

*Business continuity and disaster recovery planning are rightly higher up the agenda than in days gone by. Antony Adshead examines what 'good' looks like*

**a**ccording to the Business Continuity Institute, 20% of UK companies will suffer major disruption through fire, flood, storm, power failure, terrorism or hardware and/or software failure over the next five years. Four out of five of those, it says, will fail in the subsequent 13-months, but those that successfully restore their business will see the value of their company rise.

At worst, the result of a major disruption is that the business simply can't get running again because the job of recovery is simply too costly. In other cases the business dies a slow death as order fulfilment is hampered and customers lose faith. At the very least, a period of downtime can see costs go up by the day, with no return.

Business continuity planning is what's needed to take the sting out of such eventualities. And that should comprise detailed preparations to ensure that all aspects of the business can get up and running within a set time after disaster strikes. Not only is it good sense to have such a plan, but in some cases it may be a requirement of your auditors.

However, first it pays to be clear on the aims of your disaster recovery plan. For example, as a manufacturer, you will be producing goods and sending consignments to customers regularly. If that's disrupted, customers are likely to be on the phone wanting to know where their order is – and when competitors get word of your tribulations they'll be on the phone too, hoping to step in.

That being the case, there is no room for taking six months off to restore a plant; in that time your customers will have long gone elsewhere.

So while business continuity planning encompasses all aspects of getting your company back on its feet, restoring the IT systems – which hold the data vital to production and fulfilment of orders – has to be key to enabling you to perform core operations.

## What to do

Which begs the question, what are the key features of an IT disaster recovery plan? In systems terms everyone needs some way of backing up – that is, replicating – current and historical data and then being able to restore it onto hardware and operating environments configured to the company's operational needs. It sounds simple but a plan is necessary to state who does what and the timeframe.

The simplest form of backing up is to produce regular paper printouts. It's a rudimentary measure but if you lack access to the IT system yet can still use working plant at least you'll be able to continue production while electronic data restoration occurs. The next level up in terms of sophistication and cost is some form of electronic storage. At their most basic these will be tape drives to which you should back up data regularly. Tapes can (and should) be taken off the premises to ensure they are safe should disaster strike.



These are still basic measures, however, and don't address the possibility of a disaster taking out all data storage and processing facilities on-site. To address that you need remote back-ups via high-bandwidth network connections to a remote mirror of your storage, or to those of an outsourced provider.

### Replicate and test

Achieving reliable back-ups is the first step to restoring your systems. Next you need to be able to process the data. For this you'll need to replicate your essential hardware and software so you can restore data to it and get at least that back up and running. Again, this can be on your own assets or those of an external provider, either at a data centre you can work from or capable of delivering all you need on, for example, a 40-tonne trailer.

So, you need to back up your data and be able to process it. Again, sounds simple doesn't it? But there must also be a plan to overlay these base level actions that specifies who does what and in what order. Your plan needn't be a massive document: just a couple of pages clearly outlining the scope and timescale of IT contingency measures is better than no plan at all.

For guidance, the four key elements of planning are: rating the importance of your hardware assets, milestones towards the recovery of your systems, testing the plan and then updating it.

Rating importance of assets and generating milestones towards system recovery paid dividends for one firm – electrical products manufacturer Electrium, which has three sites in the midlands and the north west running the SSA PRMS ERP software on an IBM iSeries box, along with five Windows NT4 servers providing document management, email and file and print.

If its systems go down the company loses around £200,000 a day and IT manager Phil Robertshaw is clear about the most important components of his systems. "If one of the PC servers went down it would not be as important as the iSeries being taken out," he says. "Our plan covers the iSeries and three of the five PC servers. Email is the way our customers send orders to us, so is far more important than document management and analytics applications."

Electrium's disaster recovery provision is outsourced to ICM, and in case trouble strikes it knows it will be provided with the necessary hardware and software to get its key ERP and email up and running again. And its plans have been well and truly tested. "We're very happy with what we do and we know it works because it's been tested thoroughly by the fact that we've invoked the DR [disaster recovery] plan twice," says Robertshaw.

On one occasion the iSeries server lost power on a Sunday evening. The back-up power supply kicked in but after a while it shut down and the system closed down with it. On another occasion the Windows email server went down when some large emails overloaded the information store – which then failed to restart after Exchange was shut down. On both occasions a call to ICM put them on standby while Electrium staff worked

to get their systems back up, and in both cases ICM's mobile data centre had the company's key systems back to normal within 24 hours.

However, while testing is key to any successful DR plan, most manufacturers don't want to rely on the 'benefit' of experience like Electrium's for it. One company that does regular testing is Cheltenham-based steam control equipment manufacturer Spirax Sarco. Group IT manager Derick Brazier says: "Every November we test the disaster recovery plan and we find out what we're doing well and what needs attention. It gives the team a chance to knock the rust off the plan."

That's good, but it's also worth noting that organising tests so they reproduce likely conditions as far as possible is vital. Make sure those people responsible for elements of the plan in real life take part, and record the results so you can see how to improve things.

Spirax Sarco does exactly that. It has 1,300 UK employees at three plants using 680 PCs with HP Intel-based servers and Oracle and other vendors' SQL databases. It is also rolling out JD Edwards' Oneworld (now

**"Don't leave it to guesswork. If a real situation hits, it'll be too late"**

*Derick Brazier, Spirax Sarco*

under Oracle) ERP software internationally and uses an external provider – Sungard – for IT hosting in case of disruption.

One of its key findings has been that because the company has some legacy hardware and software, while Sungard's systems are all new, there have been situations where the company cannot run some of Spirax Sarco's applications under DR conditions. "We still run some applications on NT," explains Brazier. "There's no need for us to spend money upgrading things unnecessarily but we do have to ensure Sungard can run the software we have... Don't leave it to guesswork. If a real situation hits, it'll be too late." ■

Enter 290 at [www.mcsolutions.co.uk/enquiry](http://www.mcsolutions.co.uk/enquiry)

**Below and far left: the infamous Buncefield incident**

