FACING UP TO HARSH REALITY

THERE IS NO ROOM FOR COMPLACENCY WHEN IT COMES TO IT DISASTER RECOVERY PLANNING, PARTICULARLY IN LIGHT OF RECENT EVENTS, EXPLAINS **DAVE CLARIDGE** OF KPMG CONSULTING.

The events of 11 September have spurred many companies to re-examine their IT disaster recovery plans in the climate of increased terrorism throughout the world. The Gartner Group predicts that 40% of companies which experience a disaster will go out of business some five years later, due mainly to the cost of recovery being too high, loss of confidence from their clients or, worse still, loss of key staff. In fact, some of the financial services companies in the World Trade Centre sadly lost more than a third of their key staff, including senior executives. However, despite this new threat , we fear this renewed interest in IT disaster recovery will be only transient. This is because a large number of companies still see IT disaster recovery as an expensive insurance policy.

Here, we will examine why many companies, regardless of the world climate, still have the view "it won't happen to me". For those companies that recognise the need to take action, we will cover some of the actions necessary to reduce the chance that a disaster will cause your business to fail.

WHAT DO CIOS TYPICALLY THINK ABOUT DISASTER RECOVERY?
To many chief information officers (CIOs), IT disaster recovery sits at the bottom of their priority list compared with other IT projects such as new business functionality and e-commerce. This is because a lot of them believe that expenditure on disaster recovery will be hard to justify with the business given that the probability of a disaster on a large scale is seen as being very small. Here are some of the views we have heard from CEOs and CIOs:

- "It's not my highest priority, it's not worth spending money on it and it won't happen to me. I will deal with it when it does."
- "My insurance policy will cover me for the cost of a disaster, I don't need to spend money on back-up infrastructure now."
- "I have up-to-date technology and mirrored datacentres so have solved all the problems."

One CEO of a financial services trading company believed it wasn't worth spending money on his recovery site. This meant that disaster recovery tests were constantly cancelled and as a result the recovery site started to fall into disarray, with discarded equipment and general rubbish stored in it. When the CEO was asked why he wasn't concerned about the recovery site, he merely answered that "the IT boys can fix all that once the disaster has occurred."

There are common trends in the way IT disaster recovery is treated in terms of processes. To follow, we will explore some of the these and highlight the issues that could arise as a result.

RECOVERY FACILITIES. Most big financial services companies tend to handle disaster recovery in-house rather than outsource to a specialist provider. The method used will typically be some form of secondary data centre containing back-up IT infrastructure – for example, servers, network components and printing. Usually, back-ups of data at the primary datacentre are carried out each night and stored in a fire safe and at some point transferred to the back-up site, dependent on policy. Often companies that use duplicate IT infrastructure in a back-up datacentre are tempted to use this equipment in the production line datacentre when some sort of hardware failure has occurred. Once the infrastructure at primary and back-up datecentres goes out of synchronisation it rarely gets back in sync again and the disaster recovery strategy is compromised.

A few companies still have primary and secondary datacentres on the same site. Based on the World Trade Centre experience and many other disasters, such as the Canary Wharf bomb in London's Docklands, emergency services will be reluctant to allow you to go into the disaster area for some time after the site has been made safe. So access, even to an undamaged back-up site on the same campus, may not be possible for many hours, or even days, and your recovery will be seriously jeopardised.

There are also significant issues with any strategy that involves backing up data to tape at a primary site and then transferring it to a back-up site where it can be later recovered. The process of backing up and transporting data on tape is fraught with problems and requires very careful management. A very common issue cited on a lot of failed tests is that tapes required for a disaster recovery test have gone missing. Unless these back-up and tape management processes are both rigorous and frequently tested they represent a real threat to the ability of the IT disaster recovery team to recover all critical business data.

'FIRMS AND DISASTER RECOVERY VENDORS FREQUENTLY FAIL TO DEVELOP THE PARTNERSHIP NEEDED AND THE SUPPLIER BECOMES CONTRIBUTORY TO FAILED TESTS'

A few companies may use an outsourced service for disaster recovery and business continuity. Outsourcing, if used effectively, is a strong solution for disaster recovery. However, companies and disaster recovery vendors frequently fail to develop the partnership needed, and the supplier becomes contributory to failed tests. We will look at this in more detail when we cover issues surrounding disaster recovery testing later in the article.

THE RECOVERY PROCESS. In the event of a disaster, there will usually be a designated emergency management team and specialised recovery teams – for example, one team restoring critical servers, another restoring the network. Organisations often assume that the same people who provided IT support for the recovery tests, such as IT operators, operating systems specialists and database professionals, would be available in the event of a major disaster to recover the IT systems at the back-up datacentre. This clearly cannot be assumed as experience from the World Trade Centre disaster sadly confirms.

To make matters worse, the IT recovery procedures will be highly technical and require local site knowledge to be understood clearly. Therefore they would only be useful to the recovery team who had written them and unlikely to be of much help to a team of external IT contractors brought in to deal with the after-effects of a disaster where key IT staff have been lost.

DISASTER RECOVERY TESTING. In almost all cases, organisations use planned disaster recovery tests. These take the form of some sort of plan as to what will be tested – for example, recovery of the operating system and critical applications. Tests will typically be performed annually and be the responsibility of the IT department, with little, if any, business involvement.

The results of testing tend not to be distributed much outside the IT department and most tests are declared as successful, even when problems have occurred. There seems to be a common theme in that companies with disaster recovery problems all claim success with testing, even though the same problems occur again and again.

It's quite possible that each party has its own agenda in not owning up to those 'small problems'. The in-house recovery team will stick together – after all, they are the ones who put in the hard work, perhaps giving up free evenings to carry out the tests, and so are not likely to point the finger at 'Joe' for forgetting the combination to the fire safe. Also, the disaster recovery vendor may be in the situation of a test being immediately before a contract renewal point. Will the disaster recovery vendor really be prepared to report on that 'small issue' that would have led to failure on a real disaster but was ignored on the test?

To give an example, a healthcare company was running an IT disaster recovery test when they found that a tape needed for recovery was located in the primary datacentre. Unbelievably, the recovery team manager telephoned the supposed burned down datacentre and requested that the missing tape be sent out so the test could continue. The reason the tape was missing (it was due to an operator not putting a back-up tape in the tape box for offsite storage) was not considered and no plan was ever put in place to prevent this from happening again.

A short time before a planned disaster recovery test there will be a flurry of activity. Meetings with disaster recovery suppliers, internal meetings, people checking that changes made to the production IT infrastructure since the last test have been reflected at the disaster recovery site and the like. Of course, none of these activities are relevant in the event of a real disaster because real disasters are mostly not proceeded by warnings to allow such preparation.

Disaster recovery vendors used as part of outsourcing arrangements tend to contribute to this issue even more, as they will insist on a meeting a week before a test to discuss what has changed since the last one. But, in the intervening period since the last test, there will have been little, if any, communication between the two parties. Again, there is no realism in this sort of disaster recovery strategy.

So what is really being tested in planned disaster recovery tests here? The answer, unsurprisingly, seems it is purely a test of the IT department's ability to recover key data and systems, if they are given sufficient warning. This is all very well but how would the IT department handle a real situation where no such preparation would be possible?

HOW IS DISASTER RECOVERY TREATED WITHIN THE IT ORGANISATION? Disaster recovery is usually handled by individuals in the IT department who have some form of disaster recovery responsibility, typically carrying out other functions such as contingency planning or security.

There will be some form of IT recovery plan, but there may or may not be an associated business continuity plan, or the two may have been developed separately and have no linkages. IT disaster recovery will have little business involvement and tests will be organised by the IT department. Internal audit will take an interest but are likely to be phased by the technical jargon and rarely attend any such tests, preferring instead to use the tried-and-trusted interview process with IT managers.

IT disaster recovery will be seen as separate from other IT processes and will not figure in the IT life cycle. Thus the costs of disaster recovery are not considered in the investment case for new business applications, nor will ease of recovery be considered in the application design. Critically, disaster recovery is not integrated into the change management process, so changes are made to the production IT infrastructure and subsequently not to the disaster back-up datacentre, leaving the process open to failure.

USING NEW TECHNOLOGY SOLUTIONS. It is now possible for data on both disk and tape to be mirrored in real-time to a back-up site as long as this site is within a distance limit of typically about 20km to avoid performance overheads. However, some of these solutions are configured in such a way that testing that the data can actually be recovered at the remote site disrupts the production site. This means testing is either not carried out or is only done when the service can be taken down for a specified period.

The danger with any sort of technology solution for disaster recovery is that it can introduce complacency as a result of an organisation believing that once data and computer systems can be recovered the problem is over. This, as we will see later when we look at issues around loss of key skills, is far from the case. As an example, an energy distribution company which had spent large

'DISASTER RECOVERY PLANS, WHICHEVER FORM THEY TAKE, MUST USE DISASTER RECOVERY TESTS THAT TRULY SIMULATE A REAL DISASTER'

amounts of money on a strategy for mirroring a large number of mid-range servers to a remote disaster recovery site found that the solution worked perfectly apart from one problem – it was not able to test that the data could actually be recovered without taking down the whole service. Worryingly, the company ignored this issue and never tested the data recovery system, instead being convinced that the technology was 'bullet proof'.

To summarise, unless testing strategies are well designed, good recovery plans are in place and many other activities are carried out, new technology remains merely a technical solution that needs to be part of a complete disaster recovery strategy for it to be effective.

LOSS OF KEY PERSONNEL. One thing that is often overlooked is whether the critical IT staff needed to recovery the data and support the systems afterwards will survive the disaster. Unless disaster recovery plans address this issue any sophistication with technology, processes and the like will be a waste of time. This is not just confined to IT either, as loss of critical business executives in treasury and corporate finance can equally have a devastating effect on business.

RESCUE REMEDIES. Facilities for disaster recovery must be carefully considered. Primary and back-up datacentres, where used, should not be situated on the same campus or site, and not on flight paths etc. should be carefully considered when choosing facilities. Where a decision is taken to utilise a back-up datacentre, the infrastructure in the datacentre must mirror production and be maintained religiously by change management. There should be no possibility of the infrastructure in the back-up datacentre being hijacked for production usage, nor should it be used as dumping ground for old equipment.

The cost of duplicate IT infrastructure can be controlled dependent on the service levels for disaster recovery. For example, some companies may decide not to invest in expensive back-up network infrastructure but instead in the event of a disaster they will use some form of supplier managed service 'fast ship' facility for expensive production network equipment.

The use of planned disaster recovery tests cannot hope to achieve simulation of a real disaster, instead, some form of unplanned testing strategy must be put in place. These tests should be the responsibility of the business, which should call these tests randomly, without warning, to see whether IT could really recover data and systems within the timescales promised by the recovery plan.

One method used successfully by a private health company was to let internal audit be responsible for calling unplanned tests and monitoring their success. Testing must be seen as an iterative process which implies that the more unplanned tests that are run, the more that can be learned about what can go wrong in the event of a real disaster. It will also help increase confidence in the recovery process.

Every incident during a test must be reported, its root cause located and a fix applied to either process or component immediately after the test. Test failure should not be seen as negative but as an opportunity to better hone the process. Scenarios can be used in 'no warning' tests to simulate different events, for example, one test might simulate key members of the recovery team being missing and the recovery plan executed to back-fill this individual with, say, contract resources on rapid call-out arrangements.

Disaster recovery must feature as a high priority with both IT and the business. It should be part of the IT lifecycle and should be integrated into the change management and manage IT procurement management processes, as well as being considered into application design. Any change to production IT infrastructure should not be honoured by change management unless a corresponding change to disaster recovery infrastructure is also made. New IT projects that require infrastructure investment must also budget for disaster recovery facilities.

IT disaster recovery plans must be written clearly, assume no local knowledge, and should enable someone from outside the organisation to both easily understand and use them. The plans should be rigoursly tested, and the content should evolve as a result of these tests.

IT disaster recovery plans must be written to synchronise with business continuity plans. For example, business processes must be carefully considered by the IT recovery plan. It is pointless if the first thing recovered is the Customer Relationship Management (CRM) application when a workflow solution demands that the first action is the completion of a spreadsheet application. The business process flow should be used to determine the order in which systems should be recovered.

Loss of key staff is a difficult issue and any approach is a compromise. One method is to identify the critical staff, those who would be needed to recover the data, run the systems and support them afterwards. Where there are two datacentres for providing disaster back-up, plans could be made for these staff to be split across the two datacentres. Of course, the communication strategy will have to be revisited to deal with a split site IT support organisation but there are very successful large financial organisations which run exactly in this way.

The use of suppliers to provide IT recovery teams, support staff and the like, on a rapid reaction basis, can also be considered, but clearly this is expensive. Outsourcing IT disaster recovery can assist with this issue, as the supplier would probably already know how to recover the data and operate the systems, having done this as part of a test, and have support staff. Again, concise and clear recovery plans and support documentation will assist this process greatly.

CHANGE OF ATTITUDE. With the threat of terrorism likely to be prevalent for some time, organisations must re-evaluate whether there IT recovery plan would really work in a disaster situation. Senior and executive management can no longer afford to ignore IT disaster recovery and attitudes towards it need to change throughout the organisation.

Dave Claridge is a Principal Consultant at KPMG Consulting specialising in IT integration, cost reduction and IT service management and sourcingstrategies within the datacentre environment.
dave.claridge@kpmg.co.uk
www.kpmg.com