

Kenson



Business Continuity Article ... are you creating disaster ... without really knowing it?

The gap between the current approach to the implementation of ICT applications and the ability to recreate them in a disaster recovery situation is growing wider ... and is now out of the reach of many organisations. In modern multi-party networks, if the responsibility for contingency planning for business continuity is unclear ... you have created a disaster without really knowing it.

It was oh so simple then

There was a time when disaster recovery was relatively easy. Take regular system backups and keep them off-site. Establish alternative facilities for users and hosts. Restore the information, processes and communications and off you go. Disaster Recovery (DR) as a process was well appreciated and understood and business continuity plans would function with a high degree of certainty and confidence. Ah! ... remember the good old days! Life was so much simpler before the advent of distributed servers, thin and thick clients, middleware and a whole raft of dependencies you never knew you had.

Two months ago, I was visiting a client where multi-party outsourcing has taken place. In the meeting it was revealed that, in the event of the data centre being un-useable, the server specialist would fall back on their DR site, the Unix specialist would do likewise to their site, and the WAN provider would link the two. Apparently fine, but the devil is in the detail. Unfortunately, the WAN provider had not been made fully aware of this plan. To add to the problem, many of the NT boxes are front end processors for data on the Unix systems, the WAN bandwidth required for this solution would be in excess of 2Tbits/sec.

Kenson Network Engineering Ltd

Corinium House
Units 101/102
Cirencester Business Park
Love Lane
Cirencester
Gloucestershire
GL7 1XD

T: +44 (0)1285 647900
F: +44 (0)1285 643686
E: enquiries@kenson.co.uk
W: www.nut.eu.com/kenson

Nu Technologies

Kenson are part of the
Nu Technologies Group

Where the buck stops

When Business Continuity is at stake, matters are not helped by re-viewing contracts and apportioning blame. In the final analysis the Business Continuity Programme (BCP) is a customer management essential to be fully supported by all parties involved in the delivery of the ICT service. For the Financial Community, the recent revision of the FSA regulations makes the responsibility very clear, *'enterprises are responsible for ensuring that they have adequate contingency plans to meet their obligations under the 1998 FSA act'*. In other words, if the responsibility for any of the delivery systems is outsourced, the organisation is assumed to have taken into account the potential risk of using third parties and ensured that adequate controls are in place.

Many clients seeking independent best practice for managing business critical networks from Kenson now realise that they have to review the DR plans of their suppliers as an inherent part of their own BCP plan. As a recent case illustrates, it should never be taken for granted. In a disaster simulation arranged by Kenson to test a client's BCP, the outsourcer could not locate the back-up ISDN connection in their data centre. The all-important local knowledge had been lost when a network specialist had been redeployed. It is scant excuse that over 200 ISDN2 are installed, particularly when most were lying loose and unidentified at the bottom of equipment cabinets. Taking two weeks to locate the right one was difficult enough to explain, it would have been impossible in a real disaster.

Driven to disaster

The move to intranet-based and distributed computing has had many benefits for enterprises, particularly the ability to integrate key business processes through the use of ICT.

The speed of change required of ICT by the business could not be met without moving to applications that are developed quickly and made available on the desktop - or as in many cases now, the laptop.

This is often achieved by designing applications that have, for example, front-end systems manipulating data held by back-ends or mainframes, thin clients accessing server farms, or information feeds being filtered and presented with interpretation etc. Enterprises have received the business benefits but experienced IT managers know that rapid change is difficult to manage and this is now one of the key drivers for outsourcing various aspects of IT.

The change is so rapid that risk awareness and contingency planning is often out of focus. The situation is getting worse, with many ICT managers not even realising the gaps that are appearing in their BCP plans and often relying upon technical specialists to identify potential management problems. In practice, a disaster or two is often needed to remind them of the value of risk management. This is a business not a technology decision and sound judgement is required to deliver the required level of cover. After the horse has bolted perhaps, but it is worth noting that a post-disaster review will normally be carried out by the insurers - who will be looking to see that you minimised losses by adequate planning.

Lifeline

The BCP life cycle shown is fairly standard in nature. Project initiation being relatively straight forward, the functional requirements phase is where it gets more difficult as you have to start gathering facts about the business units and the IT systems that support them. The problem with DR and BCP planning in modern environments is that the information you would expect to have easily available often doesn't exist. *'Who should own the ICT documentation?'* is always an interesting question. *'Who should maintain it?'* is more interesting. How they maintain it and guarantee it, is a subject often debated with no conclusion. Look at the immense efforts required in Y2K programmes to identify critical business processes, the applications, the systems that underpin them and the dependencies that have to be understood. BCP is almost like an ongoing Y2K programme, it is a management task that should be part of normal day- to-day ICT operations. As the project develops it is often the case that the BCP team become the only individuals who begin to comprehend the business importance attached to certain applications or systems.

The more seasoned ICT professionals will recognise that this has all happened before. The increased use of mainframe computing once generated the need for processes to ensure reliable service with plans on how to manage change and disaster. It has taken over 20 years for the adoption of ITIL best practices to be understood in some companies, whereas distributed network environments (DNE) are new and evolve with each new introduction of desktop & server technology.

To look at it from another perspective, BCP and DR are complex management decisions. It is difficult to assess the value of BCP and then spend money today on plans you might never invoke, especially when compared to the instant and tangible value provided by a new server or upgrading desktops.

BCP and DR are not alone, there are other ICT management needs that are being compromised by the difficulty in getting information on existing IT systems. For example;

1. Billing of outsource contracts where pricing is based on desktops or network points
2. Billing reconciliation on WAN circuits
3. Review of maintenance contracts
4. Contract re-negotiation with existing & other suppliers
5. Technology refresh estimates
6. Incident management
7. Review and update of BCP & DR plans
8. Project discovery time & implementation plans
9. Assessing single points of failure
10. Central management tools being maintained with changes

Items 1 to 6 have direct cost implications that can normally be assessed in monetary value. The larger the organisation, the greater the number of suppliers, there is naturally greater difficulty in ensuring the bills are accurate. Where the ICT department is spending money directly every year, it has a responsibility to make sure the bills are accurate, or consolidated among fewer suppliers to reduce costs - maintenance contracts are a good example. Items 7 to 10 are indirect costs in that the management task takes longer, is less efficient and the risk is increased due to lack of time or resource to make up for the difference.

The difficulty with DR & BCP planning is that it needs best practices and controls to be in place beforehand to make it easy to maintain. The same practices and controls often give more direct beneficial value to day-to-day operational needs than the management processes such as contingency planning. So the answer is simple, spend time improving the operational processes and make them people independent, and it becomes easier to plan how to overcome disaster without incurring too much additional costs. Follow best practice guidelines, where the BCP team has an influence.

If the customer is responsible for his BCP plan, why should the outsourcer incur extra costs in helping the management need of their customer, when the contract awarded was based mainly around operational costs and service levels? Did the customer or the previous outsourcer pass across adequate records? Was it written into the contract that they should be maintained? Are internal records such as BCP or DR intellectual property which should not be shared between competing suppliers, even though they are together providing components of a service for their mutual customer? In practice (generally) customers and suppliers are often reluctant to share information openly, which doesn't help the BCP programme manager.

While outsourcing often gives access to well developed supplier processes, BCP responsibility should be identified early on contract negotiations. This ensures both the customer and their partner recognise their responsibility and who owns and maintains the information. One of the benefits of outsourcing is that these issues have to be made clear to allow the contracts to work well, whereas internal only IT sourcing often relegate it to a low priority because it is difficult and often requires procedural change.

In summary, are you certain your BCP plan is not harbouring an end-to-end disaster, rather than a coordinated approach to recovery from one?

**Kenson Network
Engineering Ltd**

Corinium House
Units 101/102
Cirencester Business Park
Love Lane
Cirencester
Gloucestershire
GL7 1XD

T: +44 (0)1285 647900
F: +44 (0)1285 643686
E: enquiries@kenson.co.uk
W: www.nut.eu.com/kenson

 **Nu Technologies**

Kenson are part of the
Nu Technologies Group