

HOW MUCH DO YOU REALLY KNOW ABOUT OFF SITE RECOVERY?

Author: Mike Osbourne MBCI, Operations Director, ICM Recovery Services. Published in Continuity Volume 9 issue 4

The bombings in London in July '05 brought the issue of business continuity once again into the spotlight.

As the first sustained terrorist threat in the UK since the IRA strikes of the 1990s, companies experienced at first hand the threat of wide-area terrorism to their businesses.

Clearly this is an issue that simply cannot be ignored but, perhaps more importantly, last year's events have revealed a number of new challenges that businesses had not previously thought about when it comes to continuity arrangements.

Until a few months ago many companies considered themselves to be up to date with business continuity, with sufficient plans in place. Now they are finding that these plans need to be reviewed to consider factors above and beyond those raised by a conventional attack.

For example, can recovery organisations guarantee sufficient capacity to support multiple invocations from businesses across a large area?

With so many honed continuity plans there were a significant number of clients who placed their third party business continuity contracts on standby or even 'invoked' on 7 July.

Invoke or sit tight?

Many of these were not directly affected by the incident but invoked on the basis of the perceived threat. The 'Continuity Central' web site estimates that there were at least 106 standbys and 29 invocations following the bombings.

This raises the issue of what would happen if organisations invoke because of a perceived threat, and by doing so impact the recovery ability of businesses that are actually affected? This particularly applies to syndicated services that have high subscription ratios, or operate an equitable sharing scheme that may see available space divided among the 'standby' and actual invocations.

This leads us on to what is becoming a hotly debated issue in the industry – the responsibility of providers to be 'transparent' to their clients when it comes to syndication rates.

Following the bombings, the Tripartite Authorities – made up of the Bank of England, The Treasury and Financial Services Authority – issued an incident review report.

While the survey did not address the issue of syndication rates directly, there was some concern expressed from organisations over the level of subscription for individual sites, in particular issues around prioritisation and space sharing in the event of multiple occupations.

This is not the first time this issue has been mentioned and it is something the FSA has talking about since the events of 9/11 in New York.

In simple terms, over-subscription of a business continuity service can leave clients unable to adequately test a plan, and can even leave them fighting for space in the event of a wide area-affecting incident, potentially rendering a contingency plan invalid.

An ideal arrangement would be to opt for a dedicated recovery seat, but this is an expensive option.

Shared v dedicated space

A dedicated seat – which is often built to order in a pre-planned suite and sold on completion of build – if sold to a single client would typically cost £4,500 a year. On the other hand a syndicated seat – which would be sold to multiple clients – would cost in the region of £350 a year.

In order to achieve the same level of returns equal to a dedicated seat, it is therefore necessary for business continuity providers to sell a number of seats over and over.

However, it is important that clients are informed of these subscription rates when signing up to a provider, to ensure they are fully aware of the level of service to expect. Clearly, in the event of a wide-area incident, if a number of companies in the same geographic area are contracted to the same provider, they may be left competing for the same recovery seats.

The general industry ratio for selling seats is anything between 40-1 and 25-1, i.e. each desk is sold a maximum of up to 40 times.

The Business Continuity Institute's Good Practice Guide states: "Great care should be taken to understand who are the other customers potentially using each desk" and in response to this, some suppliers provide client details by postcode. The distance within which the recovery supplier will not resell the resources you have subscribed, to another potential customer, known as an exclusion zone, needs careful consideration.

For example, in the City, an 800 metre exclusion zone – the size of a vehicle bomb – is a minimum acceptable standard for this kind of threat, but clearly in light of wide-area 9/11 type incidents, it is not appropriate.

These are all important issues that business continuity providers have a responsibility to inform their customers about.

Before contracting with any provider, a firm should be fully aware of the risks of using syndicated space. The firm should also check

- the provider's back-up plans to cope with multiple invocations,
- the adequacy of the provider's exclusion zones
- and press for information regarding seat ratios.

Without this information, execution of the business continuity plan may be seriously compromised.

I believe that this is the kind of information that business continuity providers have a responsibility to provide to the customer and it is time for transparency in the industry.

Recovery providers are selling services based on trust – and trust is based on relationships and openness.

The rights of clients in terms of standby versus invocation, or the ability to invoke based on perceived rather than actual incidents are also issues the industry as a whole, or certainly individual providers need to be clear on.

SMEs are at risk

In my experience it may be the smaller firms which are most at risk as, unlike larger companies, many have not yet developed business continuity plans because the process is perceived to be complicated and expensive.

However, if syndication rates are forced down, then suppliers will need to charge more per seat. But is the market prepared to pay for this?

Once clients are armed with the full facts; price, service deliverables and risk metrics, clients will be in the position where they can decide their own risk appetite.