

# July 7<sup>th</sup> 2005: looking back for the future

Continuity Central recently conducted a survey aimed at discovering whether the events of July 7<sup>th</sup> have had a lasting impact on business continuity practices. 161 usable responses were received and they make fascinating reading. The following provides a summary of all the results.

## WHO RESPONDED?

Of the 161 respondents, 76.4 percent were from large organisations with more than 500 members of staff, 14.9 percent were from medium sized organisations (100 to 499 members of staff) and 8.7 percent were from small organisations (less than 100 members of staff). The top sector represented was the finance sector, with 24.2 percent of respondents being financial services organisations, 7.5 percent being from the banking sector, and 6.2 percent from insurance. This was followed by the public sector (16.1 percent of respondents), utilities companies, including energy suppliers and telecoms suppliers (6.8 percent) and computer software and services (6.2 percent). Many other sectors contributed less than 5 percent of respondents to the survey.

## BUSINESS CONTINUITY STATUS

A series of questions were asked to determine how prevalent business continuity planning was within the respondent population. Only 5 percent of respondents reported that they do not have a current business continuity plan. The remaining 95 percent all do. However, some of these are fairly recent developments, with 12.5 percent saying that they developed their business continuity plan after the events of July 7<sup>th</sup> 2005.

## BUSINESS CONTINUITY PLANS AND JULY 7<sup>TH</sup>

A surprisingly high number of respondents had to use either all or part of their business continuity plan on July 7<sup>th</sup>. Overall, 45 percent of those reporting that they had a BCP in place activated elements of their plan and it seems that in most cases the business continuity plan performed very well. A very encouraging 90 percent of respondents who had used their plan reported that they were either 'very pleased' (35 percent) or 'somewhat pleased' (55 percent) with the effectiveness of the business continuity plan. Only 9 percent were 'somewhat dissatisfied' and just 1 percent were 'very dissatisfied' with its effectiveness.

The survey asked respondents to provide details of how their business continuity plan was used on July 7<sup>th</sup>. The responses were as follows:

- Communication/ standby/ employee awareness.
- Full evacuation of one site - evacuation of another, but no recovery site activations.
- Had to notify staff not to travel into London. Staff affected at three key sites near Aldgate tube station.
- Some elements of the national crisis management plan were activated. The local (London) incident response team was activated to monitor and guide the continuity response. Some BC arrangements were out on standby but, in the end, were not invoked.
- We needed to confirm that our mobile staff were safe and as such we triggered a communications plan. However this did not cater for a remote incident not impacting our

premises. We have since enhanced this process with various methods whereby staff can contact a central point to inform of their safety.

- A lot of our staff were redeployed from their every day jobs to work on the response to the London bombing of 7th July 2005. This put immense pressure on the rest of our employees who had to cover the work of the reassigned staff. Where the level of staff redeployment was highest we expected departments to invoke their BC plans. In many cases the management didn't even consider these plans! Fortunately nothing happened to further stretch our capabilities and we got away with it this time. Clearly there is an awareness issue, they knew about the plan, they just didn't see its value as a tool to cover large scale loss of staff.

- Although not all sites have BC plans the general process was followed to account for all staff. We only have one or two small operations in London, however, we do make a lot of deliveries into London.

- Because our HQ is in central London and we have numerous other offices throughout the capital we were affected by the transport shut-down and had to trace missing staff, cancel meetings and await to see if other attacks followed the initial strike. Our BCP was initiated on 7/7 and 21/7/05.

- Call cascade was used and orders given in line with BCP.

- Call tree used.

- [We are a] Cat 1 responder. Provided armed protection to key assets in Central London.

- Crisis management invocation across two sites. Audio conferencing. Telephone responder.

- Crisis management plan was used.

- Crisis management elements used to manage staff roll calls, reassuring staff etc

- Cross back-up between buildings in London; crisis management procedures activated.

- Emergency communication system set up and emergency transport system put into operation. System based on Gold, Silver and Bronze.

- Event caused the crisis management team to meet. Main concerns were for staff based in London and for the pressure on the telephone network (as part of the national infrastructure.)

- Finding and locating staff.

- Finding people, making sure they were safe, call lists utilised, relocated part of work to outer London.

- Communications aspects used for contacting field staff (engineers & sales agents) working in the area and advising them of what to do in the situation.

- Incident team was invoked, as although no damage to our sites, it was unclear what was going on and if more attacks were possible. All UK staff were accounted for by early

afternoon and luckily, no casualties were reported. Plans were established to get people home if public transport did not re-open (we have a contingency arrangement with a transport provider). Incident team met virtually on Friday and over the weekend and stood down on Monday morning.

- Incident Management and Travel Policy procedures used.
- Local London office plan activated.
- Increased security presence, and took other measures in line with our plan.
- Information cascade to account for staff in London. Contingency travel arrangements for people who were due to pass through London by train to get home nationwide. Contingency accommodation for those stranded in London. Welfare for families of those affected.
- Invocation of crisis management plan.
- Invoked at Group Crisis level at head office (assessment and overall coordination) and at retail store level in London (local management of the situation).
- Invoked the Life Silver Team and used the communication call lists to ensure that all staff had been accounted for (specifically those that worked or were working in London that day).
- LCMT plan used.
- London offices evacuation/ relocation.
- Made ready our DR site and identified critical business lines. Key factor was ability to get people home/work safely.
- Made special arrangements to deal with travel disruption in the capital, and monitored staff absences the following day. Communication with staff was key. Not a full-scale activation.
- Many plans partially activated. People safety was main issue of the day.
- Not a full invocation but more a logistical issue of moving work.
- Offices based close to the events had their plans invoked.
- Only used plan in basic terms, to manage communications between other areas of the customer facing business to our people in order to manage customer and anguished relatives' expectations.
- Only in terms of communication between Board and branch managers - thence branch staff.
- Only the contacts list to confirm London based employees were safe.
- Only used part of the crisis management plan to locate staff members travelling and working in London - also to ensure we were kept up to date with what was happening.
- Our building was not directly affected but we took security advice and locked down etc.

- Monitored staff access and egress. We also provided hourly updates of the situation as we were informed, which led to a managed programme when our staff wanted to leave for the day.
- Power outage, issues with generator meant we were trying to complete the day's activities in 30 minutes; dealing with issues in CER as air-con wasn't working so needed a controlled shutdown; controlled send-home of staff; communications issues. Variety of business and crisis management activities required.
- Power was lost to our comms room resulting in the BC and DR plans having to be invoked.
- Relocated key operations to disaster recovery site on 8 July on account of fears that public transport would not be operational.
- The BCM was 1 mile from the bombings but there was not an invocation as there are deputies.
- The Incident Control Team met hourly to agree and then communicate messages to the rest of the organisation. Arrangements were made for all staff known to be in London to be identified and located.
- The plan was used to establish contact with staff temporarily working in London to reassure colleagues and families and to instruct other staff not to travel into London 7/7 and 8/7. We had to prepare to alter security arrangements. We communicated with all staff. We used the BCP to review criticality activities/recovery time scales/cascading to staff etc. Many aspects.
- Very limited references for people that couldn't travel back to London.
- We invoked the first level operational group to monitor and coordinate information and to be ready to escalate if required
- We accounted for all our staff in the UK.
- We did not use the plan but the Crisis Management Team met in anticipation of London offices being affected. They were not.
- We didn't have any sites affected, but we tried to use the plan to contact members of staff who were working in London.
- We dispatched people to our business continuity site to check functionality. Extra data was copied to external hard drive to speed relocation (no need to restore from tape). Communication plan initiated with updates on business as usual etc.
- We had a number of branches that were affected by the incident so we had to use our Branch Network Continuity plan and our Crisis Management plan to coordinate the response.
- We have 11 buildings in London and almost every one has their own BC. While not directly affected by the blast our staff travel was disrupted and we had one employee killed. As a result parts of the BC plans were used at each business.

- We have a whole raft of plans across the Group and we used the cascades contained therein to account for all staff. Luckily we didn't have to go any further.
- We invoked our Crisis Command Team Plan - no other plans were invoked.
- We invoked our crisis management plan. We also invoked our incident management plan, to deal with increased call volumes. We did staff checks in all London locations.
- We summoned Gold Team to oversee our responses as the day's events unfolded.
- Whilst we didn't invoke the plan, we adapted particular sections from it to suit our needs.

### **THIRD PARTY BUSINESS CONTINUITY SERVICES: USAGE AND PERFORMANCE**

46.5 percent of respondents make use of third party business continuity services (such as work area recovery) as an element in their business continuity response. 6 percent of these actually invoked their third-party services as a result of July 7<sup>th</sup> and 34 percent placed their business continuity services company on standby.

The business continuity services companies seem to have performed well, with 89 percent of those using their services on or around July 7<sup>th</sup> being 'very pleased' (46 percent) or 'somewhat pleased' (43 percent). Only 7 percent reported being 'somewhat dissatisfied' and just 3 percent were 'very dissatisfied'.

Respondents were asked whether they had come across any unexpected shortfalls or complications in respect of their contract cover when using their business continuity supplier on July 7<sup>th</sup>. 74 percent said that they hadn't, but 26 percent reported that, yes, various issues had come to light.

Respondents were asked if they wished to make a comment about the performance of their business continuity services company. These were as follows:

- Additional staff arrived within a few hours.
- Cover was proven to be adequate with exception of London based recovery site which was too close to restricted areas.
- HR involvement needed beefing up.
- Invoked OK, but there was a communication breakdown.
- It took some time to actually get a response from the 3rd party.
- More than one 3rd party utilised and reactions/ responses were inconsistent with pre-arranged procedures.
- Quick response from 3rd party vendor.
- Site available, although provider was busy.
- The provider was prompt in responding to our call.

- They had calls from other customers and had difficulty answering all calls, and responding to requests.
- They had changed their invocation/standby process and hadn't informed us so we had trouble placing them on standby.
- 'Deputy' was unwilling to take decisions when chief could not be immediately contacted.
- We didn't have to invoke in the end but there was a mild panic obviously because everyone was invoking at the same time!
- Went to plan.
- We were not directly impacted, hence we had to give way to others who were.
- When placing on standby we were not offered all of our work area recovery seats but we would have been offered 32 percent instead if needed to invoke.
- Worst case scenario solution not in place, therefore decided to review contract and services.

### **LEARNING THE LESSONS?**

After identifying what had actually happened on the day, the survey turned its attention to what business continuity lessons were learned from the event and how these have been implemented.

69.5 percent of respondents have reviewed their business continuity plan as a direct result of July 7<sup>th</sup>. Of these, 70 percent identified changes that should be made to their plan and 88% have turned words into action and have implemented the changes. Of those that haven't yet implemented changes, most of these report that it is as 'work in progress'.

Respondents were asked to briefly summarise what they had done to review the plan and/or what lessons they had learned. Responses were as follows:

- A 'lessons learned' document was produced and changes have been implemented.
- A review of the control and command network is being undertaken. More responsibility is being devolved to local managers in regional/local offices. Communication issues are being addressed.
- Additional communications resilience - reduce reliance on mobile phones.
- Better immediate response required.
- Catering, accommodation, transport, alternative meeting place for crisis teams, changes to travel policy and procedures for London based staff.
- Clearer communication to staff of details of event, multiple methods of updating staff, home email address, bureau service to automate text message and e-mail.

- Clearer guidance as to using the plan.
- Comms plans out of date. Staff lists out of date. Mobile phones single point of failure.
- Communication was an issue.
- Contact strategy - confirmation that people are safe required.
- Create a more detailed plan taking into account multiple issues (such as primary, secondary, and subsequent places to meet and methods for communications).
- Creation of a Crisis Communications Plan enabling remote working staff to be able to contact a central point following an incident not affecting our own premises. Methods include: ansaphone, e-mail both intranet and Internet access, direct calling. Also created a Crisis Communications Card with all relevant numbers and addresses to use.
- Crisis management and communication improvements.
- Easy access to all employees' home addresses and routes home including what public transport they use. Procedure for employees to ring home saying they are OK to save relatives ringing and clogging our lines. Better communication between teams. Increased training and awareness for all staff as well as Incident Team.
- Enhancements to communications strategy.
- Enhancing our methods of communication. Both verbally as rumours were rife amongst staff picking up snippets of information from the media. Generally people rely upon mobile telephones these days and they forgot that their desk telephone continued to work. The other factor that received some attention was how to manage the human resource aspect, people panicked when they could not contact loved ones by mobile contact.
- Ensuring that all key staff can be contacted.
- External hosting of critical applications.
- Formal plan instead of ad hoc arrangement required. The London office is adjacent to the Aldgate incident and staff were directly affected though thankfully not injured. The office was closed for 24 hours.
- Given that the tube network was out and no buses were available we had to look at ways of getting staff to the DR centre. New maps and walking directions included.
- HR and facilities plans improved.
- I developed a separate, simpler plan on how to respond to an emergency not directly affecting my employer.
- Improve communications.

- Improved IT processes to detail what can and can't be shut-down in CER as wrong things were turned off; improved procedures for manual start up of generator and improved testing schedule; stern conversation with DR provider; improved comms options.
- Improvements required for city-wide incidents.
- Incident and response communication in general, alternatives to mobiles (And update Terrorism Procedures).
- It highlighted logistical problems which were mainly communications as we have some forty sites in the London area.
- Less reliance on mobile phones. Process introduced to track staff whereabouts.
- Main areas were ability to contact staff, requirement for them to contact the office if OK but unable to come in, need for regular communications and how to deliver the messages, dealing with death of an employee - not a short term issue.
- Mainly the impact of access denial to our site by Police since we are located directly next to the main railway station in Cardiff.
- Mainly transportation issues. Also helped to review plans of companies directly affected.
- Make cascade and command and control links more prominent to more potential users. The main feature of this event was emergency responses to external issues, rather than pure BC.
- Management of contacts and messages.
- Mobile telephone communications cannot be so heavily relied upon.
- More comprehensive scoping of services which might be impacted by a remote threat. Comprehensive includes subcontractors.
- Most of the focus was upon making the plans more robust in respect of accounting for staff.
- Need for separate space for the different teams. People felt more comfortable managing the incident together, though with hindsight it may have been more effective if they were not.
- Needed to implement a specific continuity plan for London office.
- New short term DR office implemented; hardware location moved to outer London; DR office migrated to new office location in outer London; currently considering wider BCP solution.
- Nothing specific, but we are always updating following testing.
- Old BCM manager was sacked and new one (me!) employed to review and update BCM process and plans.

- Our plan relied heavily on mobile contact so we reviewed contact details and ensured we had alternative numbers for critical contacts.
- Overnight provision. More coordinated technical management procedures. A dedicated command centre.
- Plan was incomplete and suspended last year. It's now in progress again and due to be completed by end of 2006 for 35 offices. Original implementation was ill thought out. The new plan is being produced with the guidance of a BCI recognised consultant.
- Put into place emergency comms to contact all staff in an incident.
- Rather than recall all operational managers to our Hillingdon headquarters where it proved almost impossible to utilise them as a result of gridlocked Greater London roads, we now recall and disperse managers to pre determined sites around London where they are better able to respond to the needs of our business.
- Review of procedures where threat is to staff beyond phone contact (underground).
- Revision to the communications plan and our transport and operations plan.
- Sensing of the issue was good but improvement was possible. Parochial attitude of some key staff (site rather than full business view) realigned.
- Set up process for staff to contact call centre for the purposes of accounting for staff. Key supplier BC review brought forward.
- Some changes, more in relation to Incident Management procedures. Introduction of Blackberries to more key staff, upgrade of Incident Room facilities, better process for tracking staff travel.
- Some slight amends to the roles of particular individuals and not using critical numbers as a helpline as it stops other vital info getting through.
- Staff communication and awareness.
- Structure of CMT Communications processes, speed and responsibilities. Communications methods (i.e. loss of mobile). Whereabouts of staff and managers. Decision making process. Local authority contacts. Transport issues.
- Telecommunications, police liaison, board engagement, crisis management procedures.
- The plans had previously focussed on loss of property and/or facilities. We had not considered invoking them in the event of large scale reassignment of staff though we had looked at loss of staff through flu pandemic! It's about getting people to consider using their plan on every occasion where they may not be able to perform to their normal standard, whatever the cause.
- The working from home / mobile working capability was found to lack capacity in some areas of the portfolio that we would utilise in addition to 3rd party work space.

- Travel arrangements, office entry and appointment procedure. International travellers reminded of risk issues.
- Travel Plans for overseas visitors.
- We have a number of new staff who did not have a clue what they would have to do. Down to manager of each department to make sure everyone understand all aspects of the plan.
- We may be unable to rely on mobile phones or VOIP.
- We need a better one!
- We needed plans for our retail store operation at the middle level i.e. area / regional level to ensure better coordination when clusters of stores are affected in a geographical area.
- We were affected by the Birmingham Evacuation on the 9th. The cordon affected all our sites where previously we thought one to be 'safe'. Our short term contingency plans have been modified so that calls are now sent outside of Birmingham city.

### **CONCENTRATION RISK**

In the Resilience Benchmarking Project Discussion Paper (December 2005) the Financial Services Authority reported that there is a lack of transparency about work area recovery arrangements, and syndication in particular, and that this is 'causing confusion and conjecture about how arrangements might be affected by multiple invocations.' To explore the current status of this issue, respondents were asked a series of questions.

Firstly, the 46.5 percent of respondents who make use of third party business continuity services were asked: "If your primary facility is based in London, does your current business continuity plan provide for failover to a recovery centre in central London only; failover to a recovery centre outside of London only; or failover to a centre in and out of London as appropriate." The responses were as follows:

Failover to a recovery centre in central London only : 9.4 percent  
 Failover to a recovery centre outside of London only : 9.4 percent  
 Failover to centre in and out of London as appropriate : 40.5 percent  
 None of the above: 5.2 percent  
 Primary facility is not located in London: 35.5 percent

Respondents were then asked: "If you use a third-party business continuity services company for work area recovery services do you know what the maximum syndication ratio is for the services you have contracted?" Only 40 percent said that they know what the current maximum syndication ratio is. Of these the current ratios reported were:

25:1 : 36 percent  
 Between 20:1 and 24:1 : 8 percent  
 Between 15:1 and 19:1 : 20 percent  
 Between 10:1 and 14:1 : 4 percent  
 Between 5:1 and 9:1 : 16 percent  
 Dedicated facility : 16 percent

Of the 60 percent who reported that they did not know what their current maximum syndication ratio is, only 6 percent said this was because they 'don't think it is an important issue'. 42 percent said that it is an important area but that they have not yet asked their supplier about it; and 30 percent said that it is an important area but that their supplier cannot / or will not give them the information. 22 percent said that they had another reason for not knowing what their current maximum syndication ratio is. Some of these reasons were:

- It's a work in progress.
- A figure is available; I just can't lay my hands on it right now.
- That information is held by my senior manager.
- I did know the answer, which was satisfactory, but have forgotten it!
- Syndication is based on risk profile rather than maximum ratio.
- We have an exclusion zone but I will ask for clarification.
- We have asked but they have managed not to answer the question directly to date.
- We've asked, but had a very 'fudged' answer in the past.

### **RISK STATEMENTS**

In the Resilience Benchmarking Project Discussion Paper, the FSA also said that companies could gain more control over the issue of transparency by seeking an annual risk statement from their work area recovery supplier setting out how their risk profile might have changed since the previous year, including whether syndication ratios for the seats they have bought have increased or fallen.

In relation to the above respondents were asked; "Will you be asking your work area recovery supplier for a risk statement?" Answers were as follows:

I have asked for this and have received a risk statement: 11 percent  
I will be doing this within the next twelve months: 66 percent  
No, I will not be doing this: 23 percent

The latter respondents were asked to explain their reason for this response. These were as follows:

- The DR supplier would have kittens at giving away such commercially confidential information.
- Although we have an agreed ratio for seats we also know the proximity of other customers and our contract is specifically provided on an equitable share rather than 1st come 1st served basis.
- Firm not committing monies.
- Moving to internal (i.e. no 3rd Party) reliance for recovery sites.
- Our recovery solution provider has always been fully transparent with this issue and has led the field on transparency in general. We feel we have clear transparency at present although will be seeking a formal written report within the next six months.
- Our supplier is the largest in the business, with many fall-back sites.

- Reviewing DR strategy overall.
- This has recently been discussed with our recovery provider and the area we recover to is not subscribed to by many businesses in one area.
- We have skills in house (BCI) members.
- We understand our own business in sufficient detail.
- Work area recovery is a very small percentage of overall contingency planning, mostly paid direct by outsourcing customers. Our company has enough technology to allow working from any European site, or for people to work from home.

Respondents were then asked whether they had any additional comments to make on the issue of syndication. Responses were:

- We don't use it; we have a large estate and ample room to allow staff from one area to work in prearranged areas belonging to other departments. The design of our BC arrangements is that they will last for a month, during which time a recovery site will have been identified if needed. If the effect of the evacuation of the primary site is only going to last six weeks we might look to a partial return of staff to the primary site as quick as possible, to relieve the pressure on the BC fallback site.
- The big 5 should be more open and honest about how they sell each seat. And how they determine their ratio/syndication. I have heard many stories from clients who distrust the big 5 DR players!
- BC&RS are committed to dedicated targets within a certain radius mileage for work area recovery.
- I did work on this idea with our provider who was the driving force behind implementing VSD (Voluntary Service Declaration). Yet to see a statement though.
- If the supplier will not make the information transparent this is a risk that has to be mitigated i.e. go to another provider.
- If we were to have to use an alternative site, this would cause us a considerable amount of difficulty due to the alternative sites being too distant.
- It's an inherent risk. If the need is absolute certainty use own space or dedicated spaces only.
- It's how the DR companies make money, balancing the risks and probabilities of multiple invocations over large geospatial areas. I have no issues with it, but insist that we know where other companies are located.
- Our provider is able to send us to an alternative site if our primary site's syndicated seats are already in use.

- Several companies within our sector have a joint agreement with our DR supplier, who is not the biggest in the business. I have declined to join the group even though it would mean saving money as I think it is a risk too far.

- I have a tendency to suspect over subscribed facilities will only be identified if city-wide incidents occur.

- Until and unless management gets their fingers smacked, it is difficult to motivate them.

- Use of syndicated kit has to be extremely well managed and fully supported by exclusion zones, knowledge of risk exposure on such syndication and contingency in respect of such kit. To have such syndication without an "equitable share" based contract is extremely risky.

- We are currently looking to use our own buildings, i.e. town halls etc for business continuity removing the need for 3rd party locations. We would still require 3rd party for hardware only.

### **CONCENTRATION RISK**

Finally, the survey turned to the issue of concentration risk: i.e. the issue of concentration of critical sites (primary and recovery sites) within the same geographic area.

Overall, 83 percent of respondents have considered concentration risk, but only 36 percent have a formal policy in this area. Of those that do, the survey invited them to give details of what the policy was. Responses were as follows:

- As a government agency we already have covered this point by having twin office sites.

- At least 25 miles between data centres (one of which is split site with 40 metres between them!);staffing issues preclude greater distances primarily. Maximum 40 miles for work area recovery.

- Based on PAS 56.

- Based on risk assessment.

- Business recovery sites and production sites should be planned to avoid all aspects of concentration risk with regard to our facilities and other recovery facilities. This is the reason we have a two tiered approach to recovery with inner London and out of London recovery facilities available for use in an incident.

- Each department has been designated a marshalling location, most of which are more than 5 miles away from our head office. This would become a temporary office with telephone and IT provided.

- Ensuring that buildings are at least 1000km apart, no direct line of site, and not all in a cordon area.

- Fortunately, most of our offices are geographically distant but where they are not we have plans for dual invocations.

- Maybe not formal but we ensure that recovery sites are around 20 miles from our location. This reduces concentration risk but allows the people issues associated with recovery to be managed effectively.
- Minimum 40km physical separation.
- Not within a mile and not on the same flood plane no matter how far away.
- Our recovery site is four miles north of our primary site on the outskirts of the city.
- Our Strategic Management Team are located at a separate site from the Recovery Support and Divisional Support Teams.
- Primary recovery sites cannot be in the same geographical area.
- Recovery site recently moved out of London.
- Recovery site > 5 miles of primary site and no obvious infrastructure connection.
- Recovery site at least 3 miles from primary site.
- Recovery site should be more than 20 miles away and should have separate power and communication providers and transport routes should be different.
- Split / hot sites must be in place for day one critical processes.
- Split site working strategy implemented after full risks assessments.
- The policy is that this should be considered before making a decision and requires suitable sign off (MD) to accept the risk.
- UK coverage - not just local vicinity.
- We are considering up to four recovery sites throughout the UK for all our sites. They will be at least 10 miles away from any existing site.
- We are re-examining our planning assumptions and fallback options.
- We have both local recovery locations and fallback locations which are more than 15 miles from the original site.
- We have multiple sites for command and control, supply chain sources and IT data backup.
- We have one rapid response site within three miles of the main office, and a business continuity site with full functionality 80 miles outside London. Both are monitored in real-time, and data is replicated in real-time to the out of London site which is also heavily monitored.
- We have a policy that dictates minimum acceptable distances.
- We have selected buildings within our portfolio that negates concentration risk

- We know our supplier works on an equitable share basis, we also have the option of recovering to secondary remote sites should the need arise.

- We use our own sites throughout the metropolitan borough.

- When making arrangements with another department to provide fallback facilities the two parties will sign an agreement, almost like a contract. Once the agreement is reached the primary owner of the site cannot let anyone else use the agreed area as a fallback site. In this way we avoid the concentration issue by spreading the load throughout the estate. There is always the risk of a multiple attack on two or more areas but there has to come a point where the impact/probability equation reaches the point where we have to accept the risk. The only problem I could see would be in arranging to which alternative site we send the second displaced department, it isn't as though we are short of suitable alternatives.

- Where possible we try to ensure that all critical processing activities are carried out in more than one location, preferably in separate geographical areas and that there is sufficient capacity at each site to cope with the loss of one of the other sites. This is becoming increasingly difficult in light of squeezes on budget and resource.

One area which is often discussed when it comes to concentration risk is the question of how far from your primary site should a recovery facility be situated. The survey aimed to gain some real-world information on this location conundrum. Respondents who use a secondary recovery facility as part of their business continuity plan were asked to state how far the recovery facility was from the primary facility. The majority of responses were in a range from 3 miles to 39 miles:

2 miles or less: 9 percent  
3 to 5 miles: 24 percent  
6 to 10 miles: 6 percent  
10 to 19 miles: 9 percent  
20 to 29 miles: 24 percent  
30 to 39 miles: 18 percent  
40 to 49 miles: 2.5 percent  
50 to 59 miles: 2.5 percent  
Greater than 60 miles: 5 percent

Respondents were asked whether they were happy with the distance between their primary and recovery sites. 85 percent answered that they are happy that the primary and recovery site are far enough apart to avoid concentration risk. 8 percent said that their primary and recovery sites are too close and this is an issue that will be addressed in the future. The remaining 7 percent said that their primary and recovery sites are too close but concentration risk is not an issue. These latter respondents were asked to explain their answer, with the following statements being made:

- Although we believe this is not a major issue for ourselves, an equitable share contract dictates that our provider must provide facilities at the nearest available site. For ourselves this would increase travelling to around 50 miles but is feasible.

- Because of our geographic coverage we have a contingency that every one of our buildings has the ability to be a primary site and/or a primary fallback site. We then have some

locations that are also secondary fallback sites. This allows neighbouring offices to rely on each other for cover in a close proximity incident but also have coverage on the other side of town, in the event of a wider proximity incident.

- I have the option to recover to either or both of a London or outside London recovery site.

- Local recovery site in East London, host refugee arrangements within London, cross border solutions using overseas offices, out of London recovery sites in Bedfordshire and Buckinghamshire.

Continuity Central would like to thank all those who took part in this survey.