Post Event Recovery

Experience from the UK Docklands Bomb

Continuity Forum

Trailfinders

31 January 2008

Prof. Jim Norton
Senior Policy Adviser
UK Institute of Directors
Former Chief Executive
Radiocommunications Agency
www.profjimnorton.com
Agenda

Background and context.

The bombing:

- What did we do well - in advance?
- What could we have improved - in advance?
- What did we do well - afterwards?
- What could we have improved - afterwards?
- Intractable problems.

IoD survey: ICT & Business Continuity.

Final thoughts.
Background and context

At 19:02 on the evening of Friday 9th February 1996, a bomb weighing some 4000 Kilos, planted by the Provisional IRA, exploded at South Quay in London’s Docklands close to the HQ of the UK Radiocommunications Agency (RA). It marked the end of a terrorist ‘ceasefire’.

The RA (now part of Ofcom) was:

- A UK 'Next Steps' Agency created in 1990.
- Responsible for most aspects of UK civil spectrum negotiation, management and enforcement. Plus all international spectrum negotiation.
- In 1996 had 540 staff and a turnover of £40M.
- Net Running Cost regime with UK/DTI and Treasury.
- Responsible to DTI Ministers but also advises DCMS.
The extent of damage to the RA HQ Building - South Quay 3
Agenda

Background and context.

The bombing:

- What did we do well - in advance?
- What could we have improved - in advance?
- What did we do well - afterwards?
- What could we have improved - afterwards?
- Intractable problems.

IoD survey: ICT & Business Continuity.

Final thoughts.
What did we do well - in advance?

• We had worked through the disaster recovery principles with an external consulting firm (Alkemi) and thus had clear priorities for the recovery of various systems and processes.

• We had installed 'blast film' on all our windows. I believe this saved us from major casualties.

• We put in place a 'clear desk' policy, the result was little paper "blowing around" (!).

• We had largely completed the transfer of our information systems to industry standard hardware, (easy to rent replacements).

• We kept off site tape backups and a hot standby server for our key networked license system.
What could we have improved - in advance

• Cascade 'phone and address lists of all staff off site.
• Definitive list of contractors present on site.
• A network architecture without a single hub.
• Specific plans for evacuation after bomb damage and out of normal working hours:
  ▪ Access control system damaged in blast; and
  ▪ Stairwell safety plan compromised.
• Enhanced liaison with the local police. We had no idea South Quay was a designated target and we received no useful warning.
• Had more hot standby systems off site.
What did we do well - afterwards (1)

- Initial warning to Chief Executive of the explosion and immediate notifications/planning.
- Planning meeting of the Agency Management Team and advisers on the following morning (Saturday)
- Use of the Agency's 24 hour operations centre at Baldock as a coordination point.
- Extensive use of mobile 'phones to maintain initial communications.
- Departmental support to re-establish the HQ nucleus within one working day in 'spare' accommodation and to permit the use of derelict space in Companies House for us to fit out as emergency computer and licensing accommodation.
What did we do well - afterwards (2)

• Built a new networked computer centre within three working days.

• Immediate provision of counselling support for staff.

• Immediate (overnight) utilisation of existing Agency relocation team (and professional advisors) still finalising work following the move to South Quay.

• Initial press releases and internal information to staff (available from Baldock three hours after the explosion).

• Rapid identification of shortlist of potential medium term accommodation (within two working days) and rapid agreement (within two weeks) of terms on the best location - New King's Beam House.
What could we have improved - afterwards

• Greater pressure for earlier access to our bomb damaged HQ.
• More priority on the recovery of staff personal possessions - such as family pictures - after the explosion
• Off site remote download of data from SQ3 networked computer systems (which survived the blast) before power was cut off to the area.
• Improved Departmental support:
  ▪ Duty press officers were working from home over the weekend without fax facilities…
  ▪ Ministers were not informed through the Departmental process, we did this ourselves after checking.
Intractable problems

- The immense volume of unique paper in our operations (8000 crates of files went into our South Quay 3 HQ!).
- The difficulties of internal security in a shared occupancy building.
- Looking after the safety of contractors (restaurant staff, cleaners, office support staff as well as 'professional' contract staff).
- Accurately assessing the most probable threats.
Agenda

Background and context.

The bombing:

- What did we do well - in advance?
- What could we have improved - in advance?
- What did we do well - afterwards?
- What could we have improved - afterwards?
- Intractable problems.

IoD survey: ICT & Business Continuity.

Final thoughts.
Results from IoD surveys...

Small and Medium Enterprises: successful growth through ICT investment

IoD POLICY PAPER
Results drawn from detailed telephone interviews with a balanced sample of 500 IoD members

Sample by employee numbers (%):
- 1-25: 15%
- 26-50: 11%
- 51-100: 9%
- 101-200: 8%
- 201-500: 6%
- 501+: 15%

Distribution of sample by sector (%):
- Bus & Prof Servs: 39%
- Financial services: 13%
- Distribution & Hotels: 10%
- Govt, Educ, Health & Personal Servs: 17%
- Manufacturing: 17%
- Other, inc. Construction Mining & Transport: 6%

Source: IoD Dell Report: Small & Medium Enterprises: successful growth through ICT investment Sept 06
Growth ambitions of SMEs

Do you want to grow your business?

<table>
<thead>
<tr>
<th>Year</th>
<th>2004</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>92%</td>
<td>87%</td>
<td>91%</td>
</tr>
</tbody>
</table>

For those who want to grow their business, is the use of ICT a key factor in helping your business grow?

<table>
<thead>
<tr>
<th>Year</th>
<th>2004</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>84%</td>
<td>85%</td>
<td>82%</td>
</tr>
</tbody>
</table>

Percentage of SMEs as a whole who see ICT as a key factor

<table>
<thead>
<tr>
<th>Year</th>
<th>2004</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>77%</td>
<td>74%</td>
<td>75%</td>
</tr>
</tbody>
</table>

### Key reasons for investing in new ICT

<table>
<thead>
<tr>
<th>Reason</th>
<th>2007</th>
<th>2006</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase productivity</td>
<td>35%</td>
<td>42%</td>
<td>64%</td>
</tr>
<tr>
<td>Increase sales</td>
<td>16%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>Competitive pressure</td>
<td>8%</td>
<td>12%</td>
<td>3%</td>
</tr>
<tr>
<td>Save time</td>
<td>8%</td>
<td>11%</td>
<td>9%</td>
</tr>
<tr>
<td>Reduce costs</td>
<td>5%</td>
<td>2%</td>
<td>5%</td>
</tr>
<tr>
<td>Reduce risk</td>
<td>2%</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>Combination of factors</td>
<td>15%</td>
<td>9%</td>
<td>1%</td>
</tr>
</tbody>
</table>

For Mediums sized organisations, there is little variation from the total figures in 2007. Productivity is cited by 38%, increased sales by 10%, competitive pressure by 8%, time saving by 4% and reducing costs by 7%.

SMEs grow steadily more worried across a range of ICT issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>2007 Result</th>
<th>2006 Result</th>
<th>2004 Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>78%</td>
<td>68%</td>
<td>64%</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>74%</td>
<td>71%</td>
<td>54%</td>
</tr>
<tr>
<td>Spam</td>
<td>67%</td>
<td>57%</td>
<td>47%</td>
</tr>
<tr>
<td>Maintenance &amp; Support</td>
<td>57%</td>
<td>43%</td>
<td>41%</td>
</tr>
<tr>
<td>Mobility/Flexible Working</td>
<td>51%</td>
<td>30%</td>
<td>N/A</td>
</tr>
<tr>
<td>Data Storage</td>
<td>47%</td>
<td>48%</td>
<td>27%</td>
</tr>
<tr>
<td>Keeping up with Technology</td>
<td>46%</td>
<td>36%</td>
<td>21%</td>
</tr>
<tr>
<td>IT Training</td>
<td>38%</td>
<td>30%</td>
<td>13%</td>
</tr>
<tr>
<td>Setting up an online presence</td>
<td>37%</td>
<td>29%</td>
<td>12%</td>
</tr>
</tbody>
</table>

Results from IoD Dell study

SMEs: successful growth through ICT investment

• 92% of respondents agreed that they had business critical data stored in their ICT systems…

• For those with business critical data stored, 11% admitted to backing up less than once per week (if at all!). Focused in the smallest companies 1-25 employees (21%) and ‘Distribution and Hotels’ sector (29%).

• For all that back up at least once per week, 51% keep their backups on-site (18% off-site and 31% both off-site & on-site). Worst sector for keeping backups just on-site was ‘Government, Education, Health and Personal Services’ - 72%.

Source: IoD Dell Report: Small & Medium Enterprises: successful growth through ICT investment Sept 06
Agenda

Background and context.

The bombing:

- What did we do well - in advance?
- What could we have improved - in advance?
- What did we do well - afterwards?
- What could we have improved - afterwards?
- Intractable problems.

IoD survey: ICT & Business Continuity.

Final thoughts.
The identification, management and control of risk is at the heart of all successful businesses.

Businesses cannot survive, let alone prosper, without taking risks…

Ensuring that proper risk assessment and control processes are in place and working is a key responsibility of the Board.

Responsibility for identifying and managing risk and ensuring continuity of business is pervasive throughout an organisation.

BS2599 provides the necessary framework for maintaining resilience, applicable to organisations of all sizes and sectors.
But remember, managing business continuity is a continual battle. Don’t ever sit back and believe that you have won!

Oh dear…!