What is your risk appetite…?

Presentation to the:
IoD Managing Risk for SME’s Conference

One Whitehall Place, London
13th November 2007

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

Issues to be covered

• Background and context - Docklands 1996.
• Setting the scene - risk is crucial to business.
• IoD survey: ICT & Business Continuity.
• Directors’ Dilemmas.
• Continuity planning is not optional:
  • duties under legislation; and
  • duties on listed companies.
• 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 was:

- 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.
- Ultimately absorbed into Ofcom following the Communications Act 2003…

**The extent of damage to the RA HQ Building - South Quay 3**

RA coped because we had a very good senior team and because we had spent time on risk & business continuity planning….
Issues to be covered

• Background and context.
• Setting the scene - risk is crucial to business.
  • IoD survey: ICT & Business Continuity.
  • Directors’ Dilemmas.
  • Continuity planning is not optional:
    • duties under legislation; and
    • duties on listed companies.
  • Final thoughts.

Setting the scene - risk is crucial to business

Risk is an essential element of business. The crux of business success is how that risk is identified, managed and controlled…
Segmenting “risk”: PEST - Political

- Red tape, tax policy, excessive costs, national lack of competitiveness.
- Instability (e.g. in countries which represent sources of supply or demand).
- Regulatory compliance, combined code, importation of Sarbanes-Oxley.

Have we thought through our priorities and potential actions if threat becomes reality?

Segmenting “risk”: PEST - Economic

- Fluctuations in demand (both up and down!);
- Exchange rate instability.
- Aggressive action by competitors (loss of margin).
- Failure to meet customer expectations.
- Major infrastructure failure (power, communications, transport,...)

Have we plans in place to handle a sudden shift in exchange rates (1£ > 2.2$)?
Segmenting “risk”: PEST - Social

- Staff dissatisfaction, union action, pension issues.
- Skill shortages, Poor perception as place to work.
- Health and safety regulation.
- Loss of staff availability due to pandemic.

Have we plans in place to manage the consequences of ‘industrial action’?

Segmenting “risk”: PEST - Technical

- Substitution (e.g. new types of product or service based on new technologies...).
- Insufficient investment in new, more efficient, processes.
- R&D targeting and efficiency.
- Contamination with a carcinogen has occurred...

Have we plans in place to manage the consequences of a major health scare related to one of our products or services?
Segmenting risk: beyond PEST…

Operational

- Poor design or product development.
- Sales channel failure.
- Supply chain vulnerability.
- Running out of cash.
- Reliability of key processes and information.
- Fraud.
- Holistic security.

Environmental

- EU Directives.
- Pollution controls.
- Pollution arbitrage.
- Emissions trading.
- Corporate social responsibility.
- Energy efficiency.
- …

We could add still more segments: regulatory, …

Issues to be covered

- Background and context.
- Setting the scene - risk is crucial to business.
- Directors’ Dilemmas.
- Continuity planning is not optional:
  - duties under legislation; and
  - duties on listed companies.
- Final thoughts.
Results from our IoD survey...

Small and Medium Enterprises:
successful growth through ICT investment

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

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

Sample by employee numbers (%)

Distribution of sample by sector (%)

Source: IoD Dell Report: Small & Medium Enterprises: successful growth through ICT investment Sept 06
Results from IoD Dell study
SMEs: successful growth through ICT investment

- Technology is still seen as key to realising ambitions for business growth. 87% of respondents wanted to grow their businesses. Of these, 85% saw ICT investment as key to facilitating that growth…

- The critical importance of ICT is now better understood. In 2006, more SMEs were more inclined to admit concerns about ICT than in 2004. In 2006 the lead concerns were Business Continuity (71%) and Data Security (68%).

- 28% of respondents admitted to having no ICT business continuity or disaster recovery plans in place. This was predominately amongst the smallest companies, 1-25 employees (43%), in the Midlands (34%) and in the ‘Distribution & Hotels’ sector (42%).

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

---

IoD Members are more worried across a broad range of ICT issues…

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>2006 RESULT</th>
<th>2004 RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity</td>
<td>71%</td>
<td>54%</td>
</tr>
<tr>
<td>Data security</td>
<td>68%</td>
<td>64%</td>
</tr>
<tr>
<td>Spam</td>
<td>57%</td>
<td>47%</td>
</tr>
<tr>
<td>Data storage</td>
<td>48%</td>
<td>27%</td>
</tr>
<tr>
<td>Maintenance and support</td>
<td>43%</td>
<td>41%</td>
</tr>
<tr>
<td>Keeping up with technology</td>
<td>36%</td>
<td>21%</td>
</tr>
<tr>
<td>IT training</td>
<td>30%</td>
<td>13%</td>
</tr>
<tr>
<td>Mobile/flexible working</td>
<td>30%</td>
<td>N/A</td>
</tr>
<tr>
<td>Set up online presence</td>
<td>29%</td>
<td>12%</td>
</tr>
</tbody>
</table>

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

Issues to be covered

- Background and context.
- Setting the scene - risk is crucial to business.
- Directors’ Dilemmas.
  - Continuity planning is not optional:
    - duties under legislation; and
    - duties on listed companies.
- Final thoughts.
Directors’ Dilemmas

*Daring but careful*

The board must be simultaneously entrepreneurial and drive the business forward while keeping it under prudent control.

*Combine intimate knowledge with a hands-off approach*

The board is required to be sufficiently knowledgeable about the workings of a company, to be answerable for its actions, yet able to stand back from the day-to-day management of the company and retain an objective, long-term view.

*Act local, think global*

The board must be knowledgeable about “local” issues and yet be aware of potential or actual non-local, increasingly international, competitive and other influences.

Source: IoD “Standards for the Board” 2001

---

Issues to be covered

- Background and context.
- Setting the scene - risk is crucial to business.
- Directors’ Dilemmas.
- Continuity planning is not optional:
  - duties under legislation; and
  - duties on listed companies.
- Final thoughts.
Directors’ “Combined Code” duties...

Risk: … directors should satisfy themselves that the financial information is accurate and that financial controls and systems of risk management are robust and defensible.

Source: Combined Code 2003

Financial Services Authority: Handbook “Principles”

Principle 2: “Skill, care and diligence”:
A firm must conduct its business with due skill, care and diligence.

Principle 3: “Management and control”:
A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

Source: FSA Handbook online 2nd December 2006
Civil Contingencies Act 2004

The Civil Contingencies Act (2004) establishes a legislative framework for emergency planning arrangements at the local level. The Act requires Category 2 responders, many of whom are private sector bodies (e.g. utilities, transport companies), to co-operate and share information with Category 1 responders (e.g. emergency services and local authorities) to inform multi-agency planning frameworks...

Source: Civil Contingencies Secretariat: http://www.ukresilience.info/index.shtml

BS25999 represents a major step forward...

BS25999 provides the necessary context within which business continuity management can be appropriately implemented, including:

- prioritisation of activities;
- evaluating a range of strategies;
- developing the correct responses;
- testing and exercising; and
- embedding BCM into the organisation’s culture and values at all levels....

Source: BSI BS25999
Issues to be covered

• Background and context.
• Setting the scene - risk is crucial to business.
• IoD survey: ICT & Business Continuity.
• Directors’ Dilemmas.
• Continuity planning is not optional:
  • duties under legislation; and
  • duties on listed companies.
• Final thoughts.

Some 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
• BS25999 provides the necessary framework for maintaining resilience, applicable to organisations of all sizes and sectors.
But remember, managing risk is a continual battle. Don’t ever sit back and believe that you have won!

Additional slides
Experience from Docklands 1996
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 counseling 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.