
Business Continuity Research



Business Continuity Institute

Sponsored by

HITACHI
DATA SYSTEMS

In association with





Business Continuity Institute

About the Business Continuity Institute

Founded in 1994, The Business Continuity Institute's mission is to promote the art and science of Business Continuity Management worldwide.

The BCI promotes the highest standards of professional competence and commercial ethics in the provision, maintenance and services for Business Continuity Management (BCM). It provides an internationally recognised Certification scheme for BCM managers and practitioners and all BCI professional members have undergone a rigorous admissions process to ensure that they are highly competent in their areas of expertise.

For further information about the BCI or this research contact:

Lorraine Darke, Membership Services Director: + 44 (0) 870 603 8783

The Business Continuity Institute, 10 Southview Park, Marsack Street, Caversham, RG4 5AF, UK.

www.thebci.org



A note from Hitachi Data Systems

Faced with regulatory requirements and unpredictable events, enterprises need to protect their data and also retain it for long periods of time. As a result, they have to put solutions and processes in place to ensure quick recovery from outages with minimal data loss and to secure data for the long term.

Hitachi believes a company's information is a strategic asset, and therefore how it is managed, secured and accessed is key to business success. That's why Hitachi Data Systems, proud sponsors of this BCI survey, offer the broadest set of Business Continuity, Disaster Recovery and Content Management solutions in the industry.



About Business Continuity, the Risk Management Expo

Business Continuity, the Risk Management Expo is the largest event of its type in Europe. Backed by leading industry associations, media and vendors, it is the definitive event dealing with all aspects of operational risk.

Running alongside business continuity for the first time in 2005 is Technology for Compliance expo. This unique exhibition is dedicated to explaining the various regulations that affect business today as well as providing technology solutions.

For further information please call 01932 566415 or visit our website www.impevents.co.uk

Introduction

This research has been commissioned by the Business Continuity Institute (BCI) in conjunction with IMP Events and sponsored by Hitachi Data Systems. March 13th – 18th March 2005 sees the 6th annual Business Continuity Awareness Week; a BCI led global initiative that aims to raise the understanding and profile of Business Continuity Management as a management discipline.

Carried out by Rosslyn Research Ltd, a specialist market research company, this research examines current attitudes towards Business Continuity Management, via a statistically robust quantitative programme backed up by in-depth interviews. 251 interviews were carried out by telephone in January and February 2005; this methodology enabled the survey to get some psychological depth as many of the questions asked were unprompted ensuring the researchers gathered a true understanding of the concept of Business Continuity Management.

Key questions considered in the research programme included:

- How do companies understand the concepts of Disaster Recovery and Business Continuity Management and the relation and difference between these concepts?
- How does Business Continuity Management differ between small, medium and large companies and between industrial sectors?
- How important is IT and telecoms Business Continuity Management and who is in the decision making chain?
- Is outsourcing becoming more, or less important as a consideration in Business Continuity Management?

Key Findings at a Glance

Nearly 70% of companies have Business Continuity plans in place. That percentage rises to over 80% in the financial and retail sectors.

Where an organisation has Business Continuity Management in place almost 60% of development and maintenance is carried out at Board level.

27% of organisations have dedicated business continuity personnel.

Business Continuity Management has emerged with a clear identity as a wide ranging management discipline and is no longer synonymous with "Disaster Recovery".

One fascinating result of this survey is how telecoms protection is almost a blind spot in the planning of many businesses. If asked to think of something adverse happening to their business, very few people spontaneously think of telecoms failure. But when directly asked, nearly all acknowledge that it's one of the gravest threats of all.

Over two-thirds of the companies surveyed do not outsource any of their core business activities. 18% outsource at least some of their IT, which is by far the most common area for outsourcing. However, only 27% of organisations actually involve themselves in helping their suppliers to develop a Business Continuity Management plan and get involved in rehearsals of the plan. Too many companies are vulnerable to a failure in their supply chain.

Only 16% of companies have a Business Continuity strategy with provision for protecting the company's reputation.

It is the big physical disasters, topped by terrorist attack (28%), that were seen as the most prominent threat to businesses in the forthcoming year.

Business Continuity Management as a Management Discipline

What is understood by “Business Continuity Management”? Tables 1 & 2

One of the main areas of enquiry for this research project was to look at how companies understand the concepts of Disaster Recovery and Business Continuity Management and the relation between these concepts. The results in Tables 1 and 2 are based on unprompted free form answers:

Table 1

“Business Continuity Management” is described as:

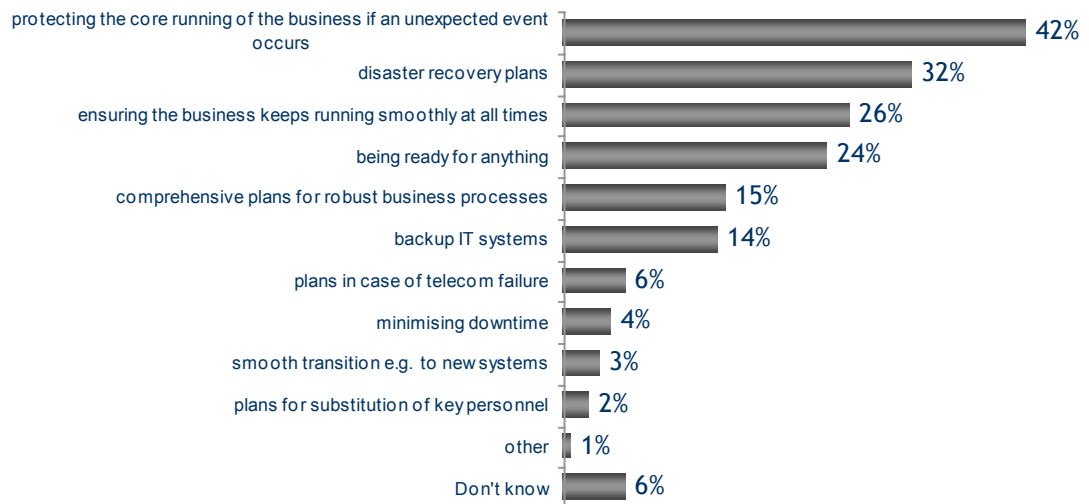
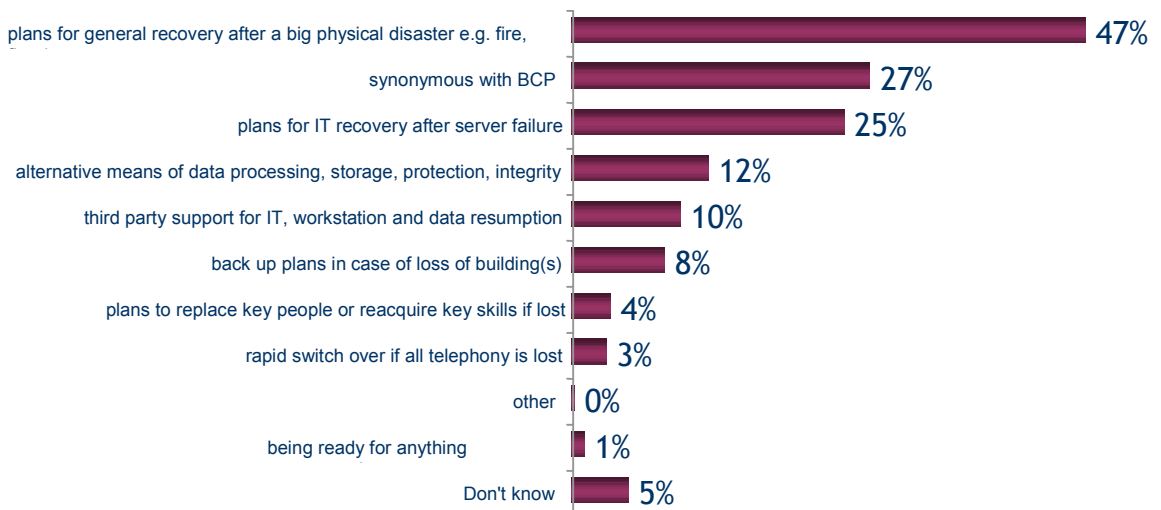


Table 2

“Disaster Recovery” is described as:



“Business Continuity” is usually described quite correctly in very general ways. “Disaster Recovery” is seen as having two distinct prime areas: IT recovery and response to major physical setbacks. It is very encouraging to see that Business Continuity Management has emerged with a clear identity as a wide ranging management discipline and is no longer synonymous with “Disaster Recovery”.

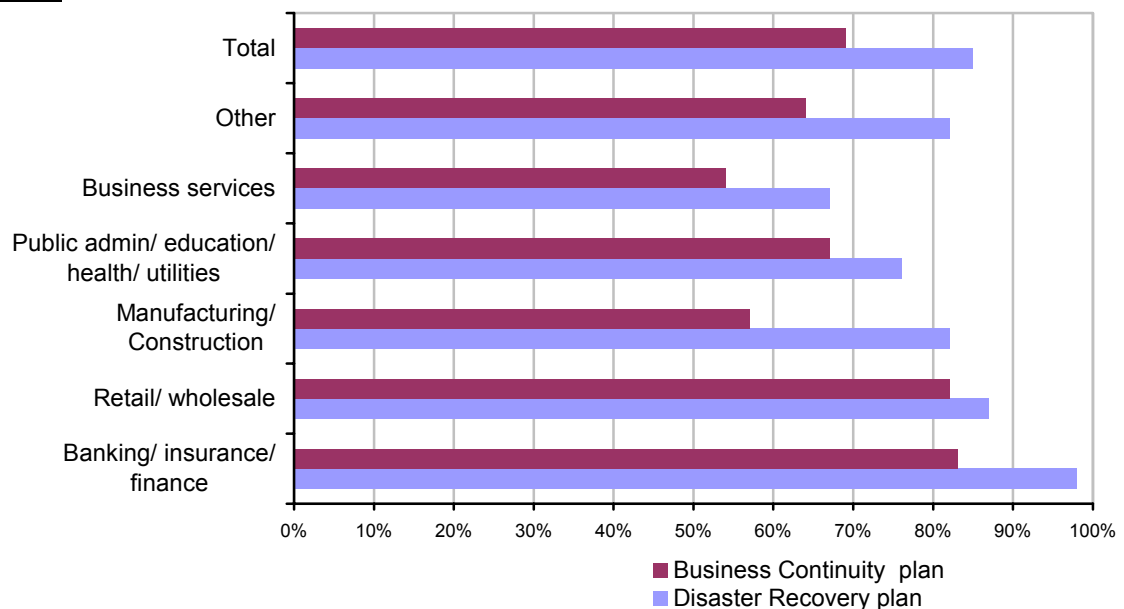
Overall it is striking how **little** association there is between either Business Continuity Management or Disaster Recovery and the issues of telecoms failure, loss of buildings or loss of key people/ key skills.

Absolutely **no** respondents make any spontaneous association with issues of reputation management or supplier failure. And yet these are all key risk areas to all businesses.

How Prevalent is Business Continuity Management and Planning? – Table 3

Respondents were asked whether they had a Disaster Recovery strategy *and* whether they had a more general Business Continuity Management strategy. Since there is some overlap between the two concepts in the minds of most of the respondents, the separate figures are broken out in Table 3 below:

Table 3



The headline figures show that more companies have specific Disaster Recovery plans than have general Business Continuity plans but that Disaster Recovery planning is always present if there is a Business Continuity plan.

Disaster Recovery is a more tightly focussed area, based around IT systems and also physical safety; Business Continuity is a wider concept which includes more of the general management issues of a business.

It is very encouraging to see that nearly 70% of companies have Business Continuity plans in place. That percentage rises to over 80% in the financial and retail sectors.

Respondents reported that it is quite rare for any aspect of a plan to have to be invoked: only 10% had to use any part of their plans over the last year.

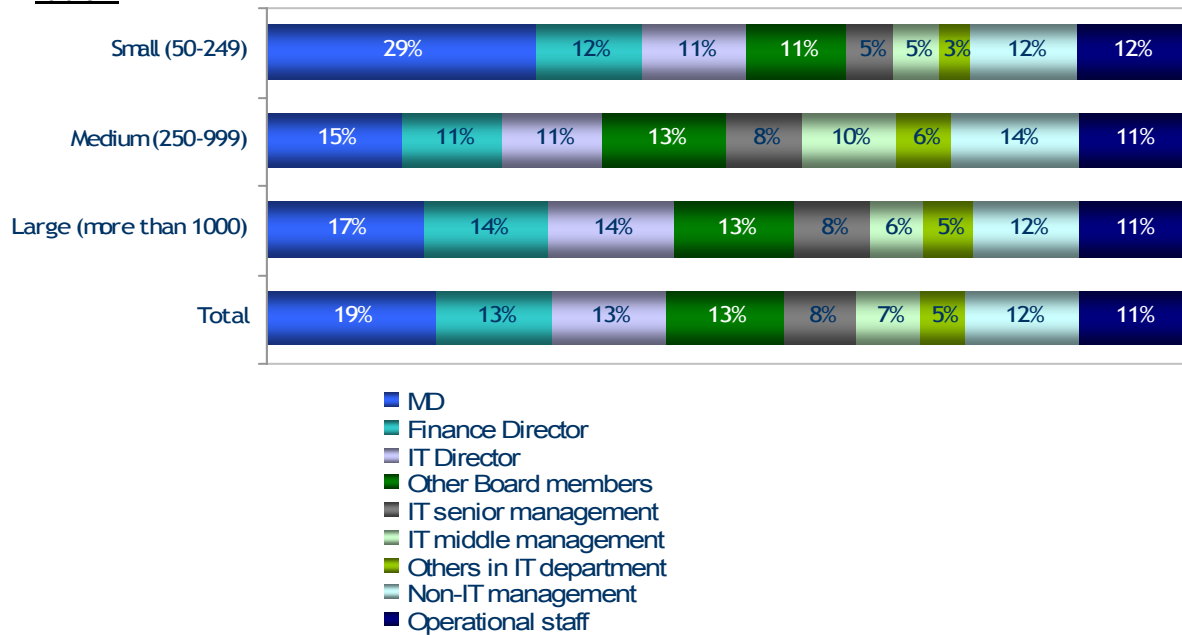
Who “owns” Business Continuity Management within an Organisation? – Table 4

Where Business Continuity Management is in place, it is developed and maintained by quite a wide range of employees. Overall, almost 60% of development and maintenance is done at **board level**. Business Continuity Management is no longer seen as an extension of IT with only 28% of IT personnel taking responsibility for Business Continuity.

17% of companies claim to rehearse some aspect of their plan every 3 months, 43% every 6 months and 6% at least once a year. The larger the company, the more frequent the rehearsal.

27% of companies have personnel dedicated to Business Continuity Management. As might be expected this was more common in larger companies. The distribution of duties is quite even across different organisation sizes, though the Managing Director personally has more influence in smaller companies.

Table 4

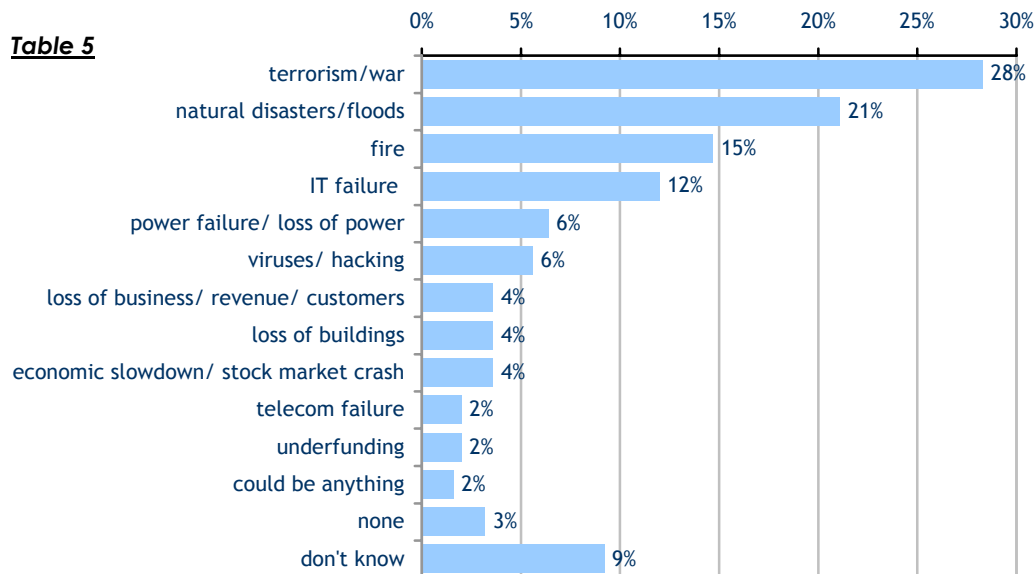


Business Continuity Management in Practice

Perceived biggest threats in the coming year – Table 5

It is the big physical disasters, topped by terrorist attack, that were seen as the most prominent threat to businesses in the forthcoming year. This may be because terrorism is the biggest media and political issue of the day which is why it springs to mind first. Terrorism appears so alarming because there is so little that an individual person or business can do about it. The need is for government guidance and information, and perhaps the very high rating of terrorist threat in this survey suggests that more could be done in terms of planning and communication to improve the resilience of civil society.

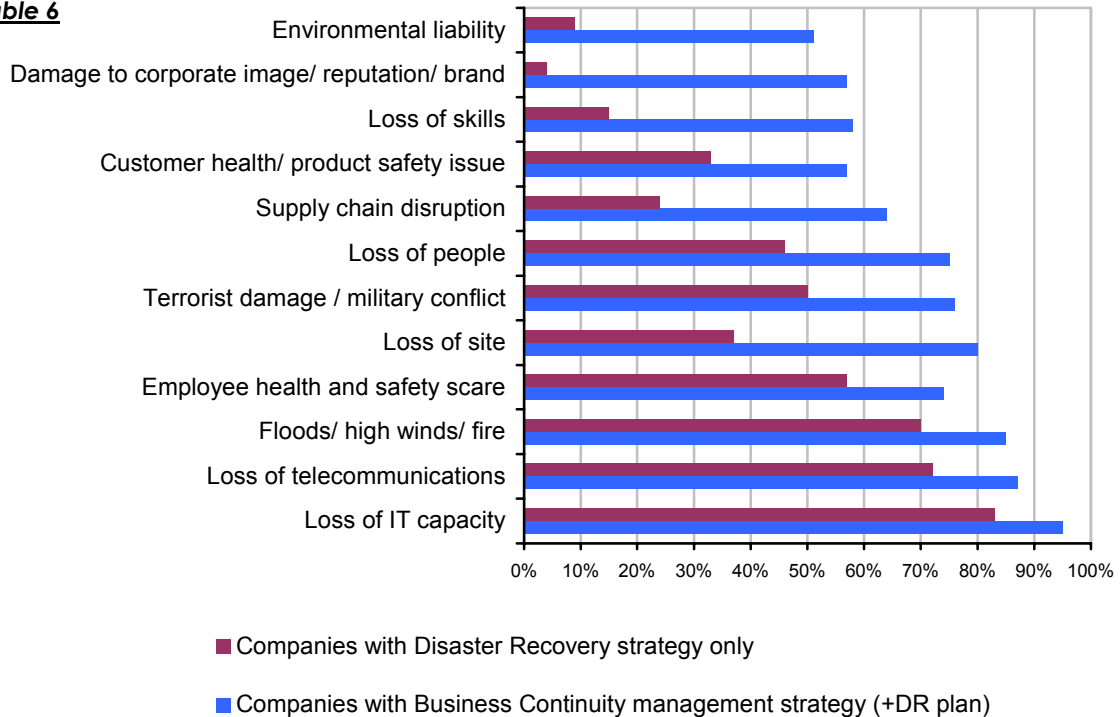
IT failure is the first "internal" threat that springs to mind. Telecoms failure comes amazingly low when people are asked to rate, unprompted, a list of possible threats.



What is covered by Business Continuity Management? – Table 6

Production of plans, both Business Continuity and Disaster Recovery, is still heavily focussed on IT and telecoms, and major physical threats. Businesses that have taken on the wider concept of Business Continuity Management rather than the narrower concept of Disaster Recovery have got far more comprehensive coverage against other, less tangible risks like damage to reputation.

Table 6



IT and Telecoms Protection

Offsite data storage (at a location managed by the same organisation) is the prime method for ensuring continuity (47% of those who claim to have protection against loss of IT capacity). Backup servers are the other main method of protection (33%). A much smaller proportion (12%) has second-line telecoms in place. 9% of organisations sampled have a 3rd-party recovery site. The risks of telecoms failure come surprisingly low on the list again. One fascinating result of this survey is how telecoms protection is almost a blind spot in the planning of many businesses. If asked to think of something adverse happening to their business, very few people spontaneously think of telecoms failure. But when directly asked, nearly all acknowledge that it's one of the gravest threats of all.

Supply Chain Protection and Outsourcing

Smaller companies tend more to rely on having a variety of suppliers; larger ones tend more to require that their suppliers have Business Continuity Management plans of their own. Overall, though, nearly a quarter have no plan to cope with disruption to their supply chain or outsourcing suppliers.

Where organisations insist on the supplier having a Business Continuity Management plan also, 18% are happy to rely on no more than a statement from the supplier. 27% ask only to read the supplier's Business Continuity plans and a further 27% don't know how the supplier's plans are verified. Only 27% actually involve themselves in helping the supplier to develop a Business Continuity Management plan and get involved in rehearsals of the plan.

This is an alarming gap in the continuity planning of many businesses. A chain is only as strong as its weakest link, and as outsourcing reaches wider and deeper, it is becoming more and more crucial to integrate continuity planning right through the supply chain.

Companies that do outsource part of their core business activities are more likely (78%) to have Business Continuity Management as a discipline in-house than those who do not outsource (65%).

Protecting Reputation

16% of respondents have a strategy with provision for protecting the company's reputation; though a much larger percentage (57%) have some sort of crisis communication plan.

This area is clearly not well planned for by many organisations. The danger of not considering systematically all the various contingencies that may threaten a company, in other words of not carrying out comprehensive Business Continuity Management, is borne out by the fact that very few organisations have considered that telecoms failure would in itself present a grave threat to their reputation *and* at the same time would make it very hard to roll out any crisis communication plan.

More than 70% of respondents agree that failure or loss of telecoms could well threaten their overall reputation; but for the most part their plans for protecting reputation are based on the assumption that telecoms are working fine.

Incentives and Drivers for Business Continuity Management – Table 7

At the historic core, which is Disaster Recovery, continuity management is a matter of preventing excessive loss from low-probability, high-impact events. In other words, it's a matter of minimising negative outcomes, and/or of simply complying with requirements from the outside (government, regulators, insurers, etc.). But as the concept develops into the management discipline of Business Continuity Management, some "pull" factors come into play – maximising productivity as well as minimising unlikely risk.

Respondents were asked to state the relative importance to their continuity management of a variety of "pull" and "push" factors. It's interesting to note that compliance comes in as only the third most important factor, not far ahead of the "pull" factor of maximising productivity:

Table 7



Evaluation of BC management processes

Amongst those who already have or plan to implement BC plans in the near future, 42% evaluate their BC management processes against external plans.

Of these almost 50% evaluate against the BSI published PAS56 and 30% against the BCI Good Practice Guidelines.

Methodology and Sample

Interviews were spread across all sectors of the UK economy and all sizes of company with 50 employees or more, with a deliberate oversampling of the financial sector.

Organisation's main area of activity

| | Frequency | Percent |
|------------------------------------|-----------|---------|
| Banking/ insurance/ finance | 84 | 34 |
| Manufacturing/production | 38 | 15 |
| Public administration / government | 33 | 13 |
| Retail/ wholesale | 23 | 9 |
| Business services | 19 | 8 |
| Construction/ engineering | 13 | 5 |
| Health | 12 | 5 |
| Distribution/ transport | 7 | 3 |
| Education/ training | 7 | 3 |
| Utilities | 5 | 2 |
| Other | 10 | 4 |

Respondents Job Title

Respondents were largely from senior management or board level. Dedicated Business Continuity Managers accounted for 10% of the sample.

| | Percent |
|-----------------------------|---------|
| | |
| Managing Director | 5% |
| IT Director | 4% |
| Finance Director | 4% |
| HR Director | 2% |
| Other Director | 10% |
| | |
| Facilities Manager | 18% |
| IT Manager | 13% |
| Other managerial role | 40% |
| | |
| Business Continuity Manager | 10% |

Size of Company

For purposes of analysis in this report, companies have been divided into three size bands according to number of employees:

| | | Frequency | Percent |
|--------|----------------|-----------|---------|
| Small | 50-149 | 20 | 16% |
| | 150-249 | 21 | |
| Medium | 250-499 | 25 | 30% |
| | 500-999 | 50 | |
| Large | 1,000 -4,999 | 55 | 54% |
| | 5,000- 9,999 | 25 | |
| | 10,000 or more | 55 | |

Conclusions and Recommendations

We are living in a very risk-conscious period. The threat of terrorism is daily occupying the media and our political processes. Understandably, terrorist attacks are the first thing that comes to mind when businesses are asked about current threats. In reality, however, companies are more likely to suffer from failure of IT and telecoms systems.

A lot of UK businesses, especially SMEs, are yet to consider the benefits of thinking briefly and systematically about all of the everyday uncertainties in their environment. The message needs to be enforced that thinking systematically about risk, and working to prevent it, is something every size of company can, and should, do. On the smallest scale, it is simply a matter of putting some structure into commonsense business practice.

Encouraging good Business Continuity Management is an area where government could contribute – not only giving direct leadership on the huge risks such as terrorism, but also helping to coordinate and communicate low-cost commonsense best practice. The Business Continuity Institute calls for the appointment of a Government Minister to promote the establishment of a Business Continuity Management Culture in the UK.