Managing Threats in a Dangerous World

The 2011 Business Continuity Management Survey

March 2011

Patrick Woodman and Paul Hutchings

Contents

Foreword

I am delighted to have the opportunity to offer some thoughts on the results of this year's Business Continuity Management Survey. And in doing this, offer the Civil Contingencies Secretariat's continuing support to this worthwhile project. I would like to thank all those that responded to the survey and, in particular, the Chartered Management Institute and survey sponsors – the Business Continuity Institute, Aon and the British Standards Institution – for all their hard work in collating the information and dispensing the results in such a clear and useful way.

We have seen for a second year that extremes of weather have caused widespread disruption amongst survey responders; in particular the cold-snap, with only eight percent of those surveyed saying that it had no effect on their business. This has meant that extreme weather has, for the second year running, been the most persistent disruptive challenge, ahead of IT failure.
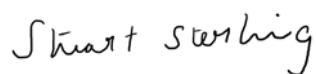
Cyber security was included in this year's survey with a third of all organisations reporting their IT systems being infected, by a virus or malicious software, in the past twelve months. This shows clearly what an important area this is for businesses to be taking steps to reduce vulnerability.

On a more positive note, however, it is satisfying to see that a high percentage of managers stated that the activation of business continuity arrangements had effectively reduced disruption. Also a number of managers said that the investment in business continuity is justified in terms of the benefit that it brings to their business, in particular, in the area of competitive advantage.

With an ever changing environment, businesses face risk on a daily basis. In the past twelve months, we have seen extreme weather, flooding, and transport disruption owing to volcanic ash. For a large number of organisations, these events have had an effect on business as usual. It is almost impossible to prepare separately for each of these risks. This is where business continuity is so valuable, allowing businesses to focus efforts and resources on the impacts that would disrupt activities; not their cause.

It is encouraging to see that organisations are acting upon information in this area, with more organisations reporting this year that they have a business continuity plan in place compared to last. In particular, there has been a notable increase in those smaller organisations that are so significant in the nation's supply chains and play such an important role in the community during a crisis. The Government is looking at ways to make business continuity more accessible for smaller organisations, and work with private sector partners to encourage its adoption.

I am sure that businesses and organisations will find this report illuminating and that, in times of intense competition for company resources, it will provide a sound evidence base to continue to invest in business continuity and promote its uptake within the supply chain.

Stuart Sterling

Stuart Sterling
Assistant Director – Corporate Resilience
Civil Contingencies Secretariat, Cabinet Office

Executive summary

- **The business case for BCM** – 84 per cent of managers whose organisations activated their Business Continuity Management (BCM) arrangements in the last 12 months agree that it effectively reduced disruption – up from 69 per cent last year. Over three quarters (77 per cent) agree that the cost of developing BCM is justified by the benefit it brings their organisation.

- **Adoption of BCM** – overall 58 per cent of managers report that their organisation has BCM in place, up from 49 per cent last year. Public sector organisations are more likely to have BCM, with 73 per cent reporting BCM arrangements, compared to 48 per cent in the private sector and 57 per cent in the not for profit sector.

- **The scope of BCM** – of those who have BCM in place, 85 per cent say their BCM includes strategies for maintaining or recovering business critical services and products in the face of disruption. Although this appears high, it is surprising that it is not higher given that this is the core of BCM.

- **Media response** – only half of those with BCM report that it includes plans for handling the media in the event of disruption, despite the fact that 61 per cent of managers agree that reputational damage is a bigger risk than financial loss.

- **Disruptive weather** – 93 per cent of managers suffered disruption in their organisation as a result of this winter's harsh weather with 35 per cent reporting major disruption. In response, staff worked remotely in 64 per cent of affected organisations.

- **Cyber and information security threats** – 62 per cent of managers report that cyber security threats are an increasingly serious risk to their business, with nearly a third of UK organisations having been affected by viruses or malicious software during the past 12 months.

- **Remote working** – remote working capabilities are becoming widespread with only 13 per cent of managers reporting that their organisation has no arrangements in place for working remotely. Over two thirds of organisations provide remote access to email, with 57 per cent reporting full remote access to IT systems.

- **Drivers of BCM** – corporate governance remains the biggest external driver of BCM with 42 per cent of managers highlighting it as a catalyst for their organisation implementing or changing BCM. Customer demands are the next biggest driver, cited by a third.

- **Testing BCM** – half of organisations with BCM exercise their plans once a year or more to test their robustness. Around a quarter fail to exercise their plans on a regular basis.

- **Training for BCM** – of those organisations with BCM, 60 per cent provide training to relevant staff. However, only one in three provide training for non-specialist staff.

1. What is Business Continuity Management?

Managers have a responsibility to ensure the continuation of business operations when an organisation faces potential disruption. Business Continuity Management (BCM) is a framework for identifying potential threats to an organisation and building organisational capability to respond to such threats, in order to safeguard the interests of key stakeholders, reputation, brand and value-adding activities.

Organisations use BCM in order to protect their people, reputation and ultimately the bottom line. The development of BCM has been supported by a British Standard for BCM, BS 25999, which provides a basis for understanding, developing and implementing BCM within an organisation. Information on BS 25999 and other resources can be found at the back of this report.

BCM is not only integral to protecting an organisation, whether from internal systems failures or external emergencies, but it also forms an essential part of the UK's wider national security arrangements. The potentially significant contribution of small and medium sized enterprises (SMEs), in particular, to communities during a disruption has been increasingly recognised. As such, the Government pledged in the Strategic Defence and Security Review, published in 2010, to support SMEs to improve BCM through a new corporate resilience programme.

The adoption of BCM in certain parts of the economy has been actively promoted by Government policy in recent years. The Civil Contingencies Act (2004) introduced a requirement for all frontline responders – such as the emergency services – to develop and maintain BCM arrangements. From 2006, the Act also placed a duty on local authorities to promote BCM to business and voluntary organisations in their communities. And in 2008, the Pitt Review on the previous year's flooding called for urgent changes to the way the UK protects itself from flooding, including the use of BCM.

The 2011 survey CMI first surveyed its members on BCM in 1999 and, since 2001, we have published an annual report on the subject. The fieldwork for this, the twelfth instalment in the series, was conducted in January and February 2011 in conjunction with Aon Risk Solutions, the British Standards Institution (BSI), the Business Continuity Institute (BCI) and the Civil Contingencies Secretariat in the Cabinet Office.

The sample was selected from CMI's membership, with 20,000 individuals sent a self-completion questionnaire, either by email or by post. A total of 1,053 responses were received (see Appendix B for details of the sample). As in previous years, the sample group represents general managers across UK organisations, rather than those with specific responsibility for BCM, and as such offers insights on how far BCM has permeated into the mainstream of business operations.

2. The extent of Business Continuity Management

2.1 Levels of Business Continuity Management

Each year the research asks managers whether their organisation has specific Business Continuity Management (BCM) arrangements covering their critical business activities. The 2011 data revealed an increase on all previous years, with 58 per cent reporting that their organisation has BCM.

It remains to be seen whether this increase is the start of an upward trend or not, but with high numbers of organisations experiencing disruption from extreme weather in recent years (as reported in Section 3), it may be that awareness and use of BCM is growing.
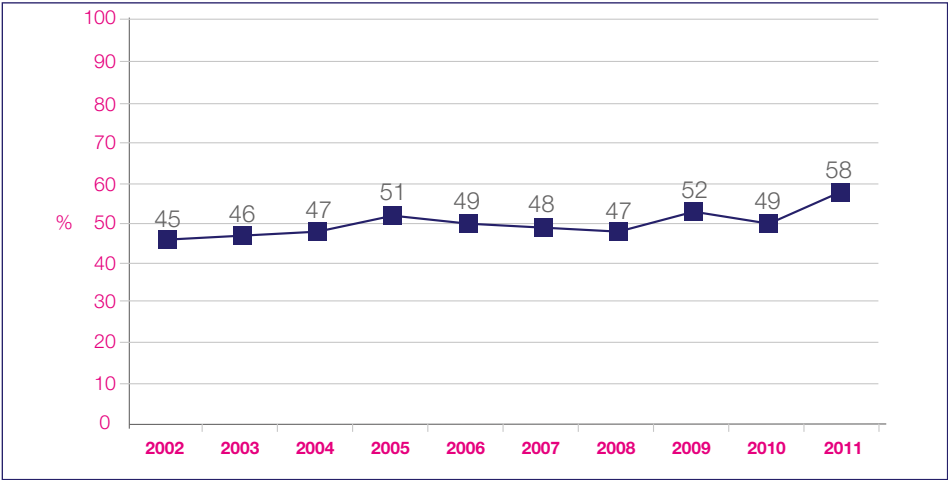

Figure 1 Organisations with BCM (2002-2011)

This apparent rise in the use of BCM is to be welcomed, but as discussed in Section 5, the evidence suggests that there are still issues about the scope and robustness of some organisations' BCM.

2.2 Variation between different types of organisation

There are substantial differences between organisations of different sizes. As shown in Figure 2 overleaf, large organisations are nearly three times more likely to have BCM than micro organisations. Nonetheless, levels appear to have increased across the sample. For example, the number of large organisations reporting BCM is up from 65 per cent last year to 71 per cent, while in medium sized organisations, the figures have risen from 49 to 58 per cent.

Policy makers have already recognised the relatively lower levels of BCM adoption among smaller organisations and pledged in the 2010 Strategic Defence and Security Review to support small and medium-sized enterprises in improving their BCM.
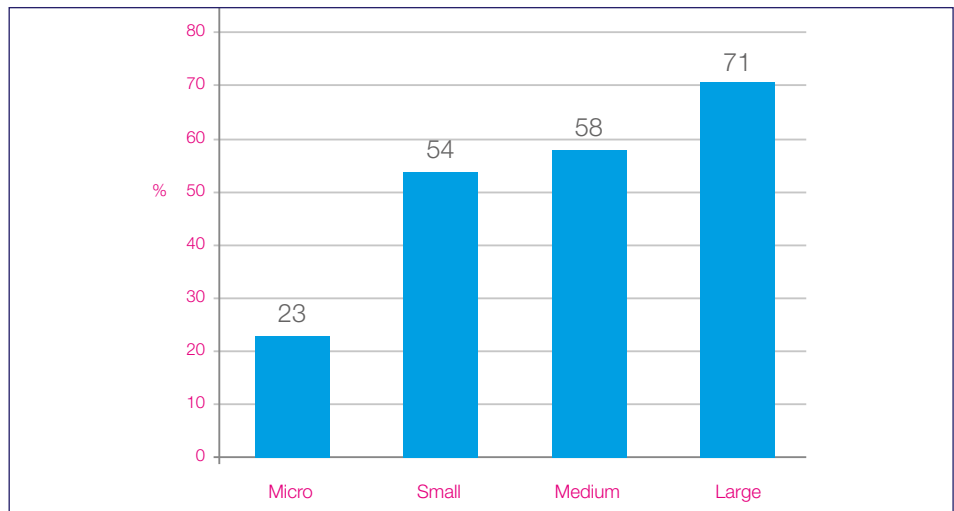
Figure 2 Organisation size[1] and BCM levels (2011)

The high proportion among large organisations is partially accounted for by the prevalence of public sector organisations in that category, which are subject to requirements such as those of the Civil Contingencies Act 2004. As Figure 3 shows, nearly three quarters of public sector organisations have BCM. While the overall figure for the private sector is 48 per cent, this partially reflects the number of small organisations in this subsample: among large private sector companies, the number rises to 68 per cent. Looking at the sector data for the last five years there appears to be a trend of increasing BCM levels, particularly in the not for profit sector.
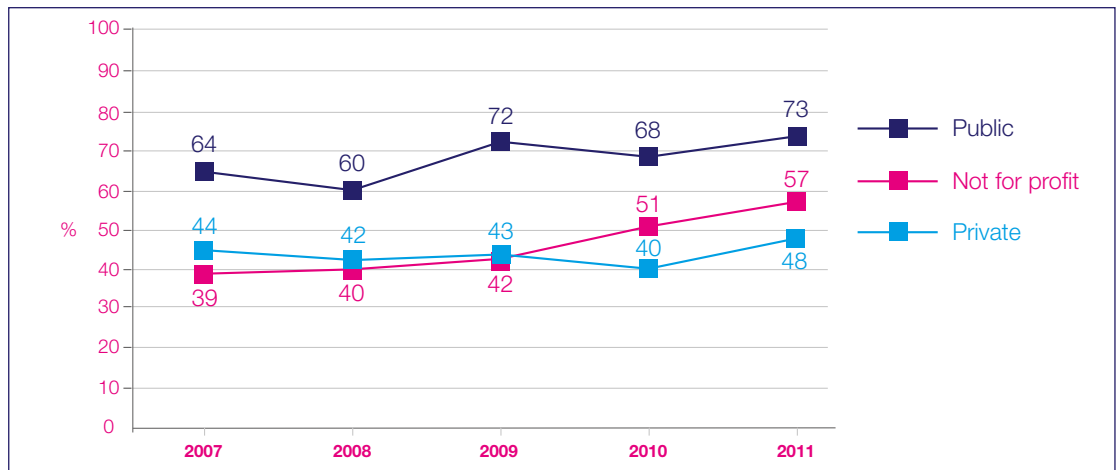
Figure 3 Organisation sector and BCM levels (2011)

There are also extensive differences between industry sectors. Only one in four organisations in the construction industry have BCM arrangements compared to 83 per cent of those in the finance or insurance sector. Relatively high levels of BCM are also found in the utilities sector (78 per cent) and health and social care (64 per cent) as well as in local government (88 per cent) and central government (87 per cent). A more detailed list with additional industry-specific statistics can be found in Appendix A at the back of this report.

1. Based on the following definitions of organisation size:
    Micro = 1-10 employees   Small = 11-50 employees
    Medium = 51-250 employees   Large = over 250 employees

2.3 Changing attitudes to BCM

The survey asks managers to assess how important BCM is considered by their senior management team. Eighty-two per cent claim BCM is regarded as either "very important" or "quite important", with 14 per cent suggesting it was "not very important" and only 3 per cent saying it is "not important at all". There remains a substantial gap between those describing continuity as important and the actual implementation of BCM.

The 2011 survey also asked managers if their attitudes have changed in light of external events such as the Deepwater Horizon oil disaster. Despite extensive coverage of the event, only 15 per cent of managers agree that the episode strengthened the case for BCM. However, the disaster placed the spotlight on the need for BCM to include PR and media strategies and, strikingly, three out of five managers regard reputational damage as a more significant risk to their organisation than financial loss.

In a similar vein, managers were asked whether the release of classified US government documents by Wikileaks had caused their organisation to review its information security arrangements. Fourteen per cent agree that it has, although this figure is higher (22 per cent) in the public sector. With Wikileaks also believed, at the time of writing, to have obtained documents relating to major US banks, the question of information security is likely to remain on the business agenda – and indeed, a majority of managers already regard cyber security as an increasingly significant risk for their organisation, as shown below.
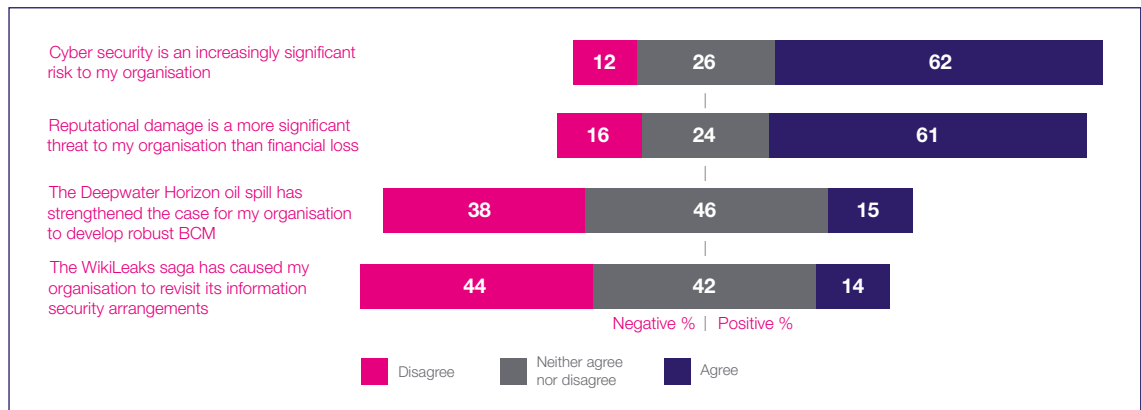

Figure 4 Attitudes to BCM issues

3. Understanding risks and potential disruption

3.1 Incidents in the last 12 months

All respondents – whether or not they have BCM – were asked whether their organisation had been disrupted by a number of specific incidents over the last 12 months. Snow, experienced both at the start and the end of 2010, caused the most extensive disruption. Over a third of managers reported that their organisation suffered major disruption as a result of this winter's weather, with 58 per cent reporting minor disruption and only 8 per cent suggesting the weather had caused no impact. Those in the retail and construction sector were particularly hard hit with over 50 per cent in these sectors reporting significant disruption.

The prominence of weather as a source of disruption was also a theme in last year's research. Climatic trends mean that harsh winters may be a more common occurrence in the coming years – which simply adds to the reasons for organisations to implement BCM.
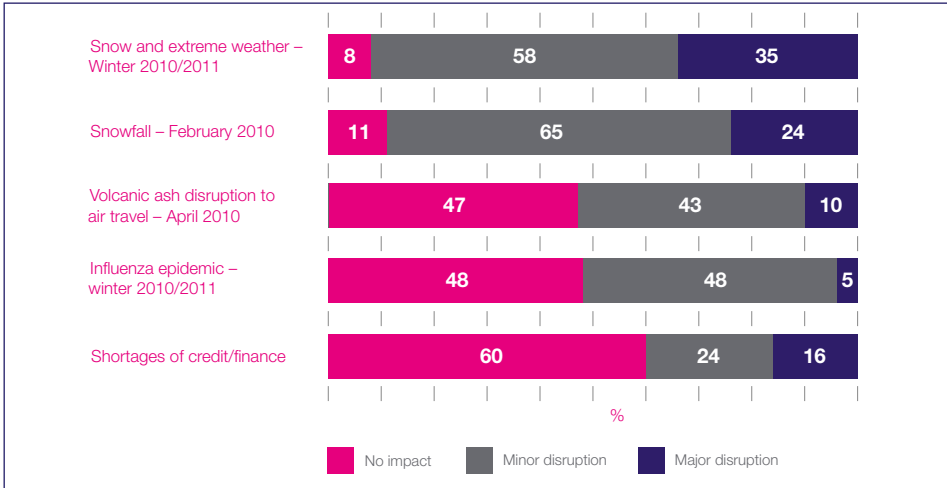

Figure 5 Impact of major incidents over the last 12 months

The eruption of the Eyjafjallajökull volcano in Iceland in April 2010 caused major disruption for one in ten organisations, rising to two in ten for multinational organisations. This year those affected by influenza was relatively small (see also Section 4.4).

With ongoing concern about businesses' access to credit, as documented in CMI's Economic Outlook research series, a question was also added on the impact of shortages of credit/finance.

3.2 Threats and disruptions

In addition to examining specific major incidents, the research examined which generic categories of disruptions have been experienced by managers over the previous 12 months. The majority of these trends have been tracked since 2002, as shown in Table 1 overleaf.

Unsurprisingly, given the effects of snow discussed above, extreme weather was the most commonly experienced disruption for the second year in a row, experienced by 64 per cent this year – more than double any other year before 2010. Transport disruption, loss of access to site and supply chain disruption were also commonly experienced disruptions that have grown in prevalence this year, factors which are likely to be linked to the weather.

Loss of IT is the second most commonly experienced disruption. The third most common disruption is a loss of people and loss of key skills is also a prominent risk, emphasising the need to address people issues in BCM and avoid a purely technological approach.

	Disruptions experienced in previous years										Covered by BCM[1]
	2002 %	2003 %	2004 %	2005 %	2006 %	2007 %	2008 %	2009 %	2010 %	2011 %	2011 %
Extreme weather e.g. flood/high winds	18	15	10	18	9	28	29	25	58	64	45
Loss of IT	19	24	25	41	38	39	43	40	35	34	52
Loss of people	-	26	20	28	29	32	35	24	28	34	35
Transport disruption	-	-	-	-	-	-	-	-	22	30	28
Loss of access to site	5	5	6	11	13	13	16	13	22	26	50
Loss of telecommunications	-	-	23	28	24	25	30	23	20	20	46
Supply chain disruption	19	11	12	10	10	13	12	9	13	19	26
Loss of key skills	33	16	14	20	19	20	21	14	15	18	30
School/childcare closures	-	-	-	-	-	-	-	-	18	17	12
Loss of electricity/gas	-	-	-	-	-	-	-	-	15	16	43
Employee health & safety incident	13	9	8	19	13	17	17	16	14	15	32
Negative publicity/coverage	24	17	16	17	16	19	18	14	9	11	20
Damage to corporate image/ reputation/brand	15	7	8	11	8	11	10	11	7	10	24
Loss of water/sewerage	-	-	-	-	-	-	-	-	6	9	36
Customer health/product safety incident	11	6	4	6	6	6	7	4	6	7	24
Environmental incident	9	5	4	7	5	6	7	7	5	7	34
Pressure group protest	10	7	7	6	7	7	6	7	6	6	13
Industrial action	-	-	-	5	6	7	7	7	4	6	20
Fire	6	5	5	5	5	6	5	5	4	4	45
Malicious cyber attack	-	-	-	-	-	-	-	-	-	4	25
Terrorist damage	2	1	1	2	3	3	3	2	1	2	35
Base: 1053 respondents (2011)											

Table 1 Disruptions experienced in the previous year, 2002-2011; and threats addressed by BCM, 2011.

1. This column indicates those respondents who have BCM covering each particular area, expressed as a percentage of all respondents.

3.3 Perceptions of threats

When asked which disruptions would have a major impact on the costs and revenues of their organisation, managers have consistently highlighted loss of IT as the top disruption, as shown in Table 2. A new item was added to the question this year, regarding the risk of malicious cyber attacks (as opposed to technical failures), and this was highlighted as significant threat by 42 per cent of managers.

Loss of access to site and loss of telecommunications were highlighted as the second and third most damaging threats to an organisation. Loss of key skills was the fourth highest result.

Despite the threat of industrial action posed by trade unions in the face of the Coalition's agenda for public sector cuts, it was ranked it 18th out of the 21 items in terms of the threat it poses to organisations.

	1999 %	2001 %	2002 %	2003 %	2004 %	2005 %	2006 %	2007 %	2008 %	2009 %	2010 %	2011 %
Loss of IT	78	82	46	58	60	70	67	73	73	71	69	67
Loss of access to site	33	55	32	54	51	53	54	60	63	55	56	56
Loss of telecommunications	-	-	-	-	62	64	56	63	68	59	62	55
Loss of skills	37	59	43	51	48	56	49	59	62	52	55	53
Fire	45	62	32	51	53	56	44	53	58	48	55	51
Loss of electricity/gas	-	-	-	-	-	-	-	-	-	-	54	51
Loss of people	-	-	-	54	48	55	56	57	59	54	52	51
Damage to corporate image/ brand/reputation	41	50	40	46	48	48	39	49	55	52	51	51
Extreme weather e.g. flood/ high winds	18	29	9	24	25	29	26	43	46	44	48	45
Terrorist damage	22	30	23	47	48	53	44	46	53	42	46	43
Negative publicity/coverage	34	43	37	45	46	44	34	43	51	41	41	42
Malicious cyber attack	-	-	-	-	-	-	-	-	-	-	-	42
Loss of water/sewage	-	-	-	-	-	-	-	-	-	-	41	36
Transport disruption	-	-	-	-	-	-	-	-	-	-	37	35
Employee health and safety incident	22	30	22	35	34	35	30	38	44	40	38	34
Supply chain disruption	-	-	25	34	32	35	28	34	37	31	36	34
Customer health/product safety incident	19	21	22	25	26	27	26	31	35	28	29	28
Environmental incident	20	19	19	26	23	35	27	30	36	31	29	27
Industrial action	-	-	-	-	-	27	22	29	26	24	29	27
School/childcare closures	-	-	-	-	-	-	-	-	-	-	17	18
Pressure group protest	7	14	9	14	27	20	16	18	27	21	19	17

Base: 1053 respondents (2011)

Table 2 Perceptions of major threats to costs and revenues

4. Understanding and responding to common risks

4.1 Effects of extreme winter weather

Winter 2010-11 was particularly cold, with December 2010 the coldest December since records began.[1] In February 2011, the Office for National Statistics blamed the weather for most of the 0.6 per cent fall in GDP in the fourth quarter of 2010.[2] In order to help understand the practical impact of the weather, the survey asked managers what impact it had on their organisation.

In three quarters of cases managers reported that the weather prevented staff coming into work and in almost two thirds of cases managers had cancelled external meetings or business trips. Supply chain disruption and reduced customer demand were also widespread, with only 8 per cent of managers reporting that their organisation suffered no effects.
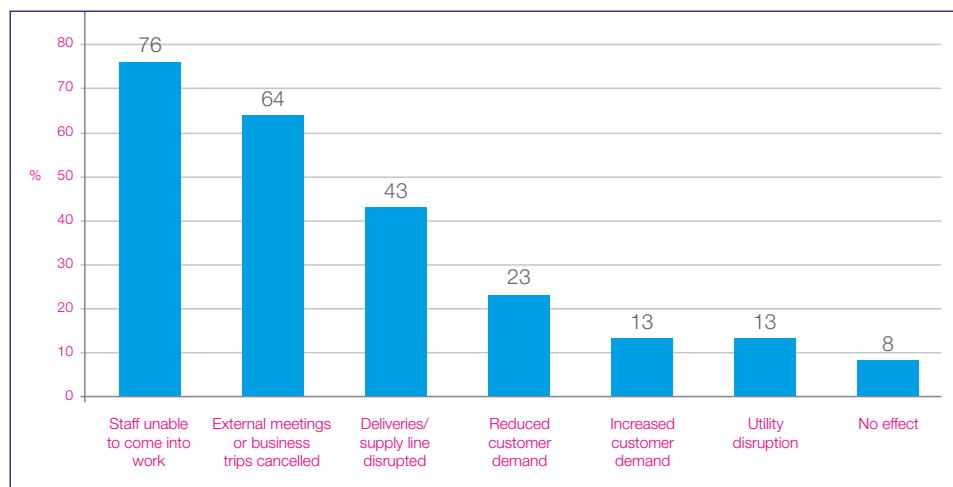
Figure 6 Effects of harsh winter weather on organisations

4.2 Responding to the extreme winter weather

Thirty per cent of respondents reported that their organisation had activated BCM arrangements in response to the harsh weather. As Figure 7 below shows, however, a more common response was remote working. Many were compelled to postpone work until the weather improved, prioritise resources on key projects or introduce overtime to make up for lost hours.
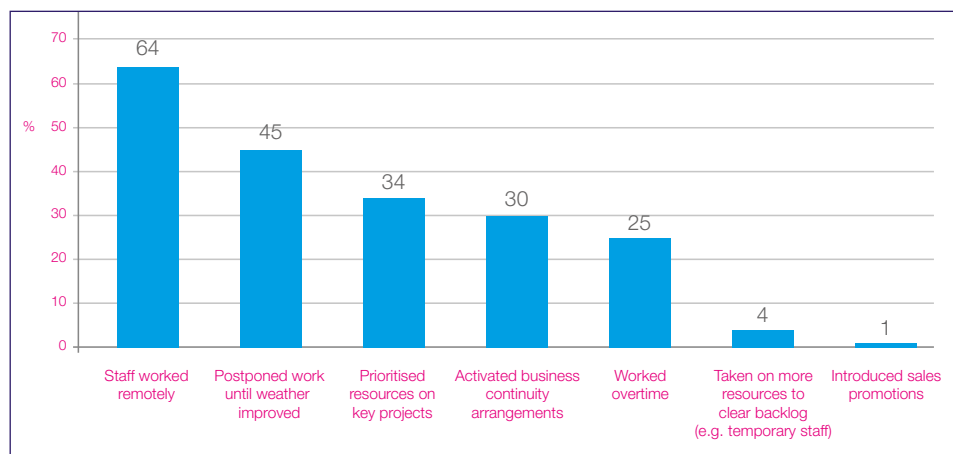
Figure 7 Steps taken in response to the harsh winter weather

1. Met Office. (2011). Record Cold December. Available at:
   http://www.metoffice.gov.uk/news/releases/archive/2011/cold-dec
2. Office for National Statistics. (2011). GDP Growth UK Output decreases by 0.5%.
   Available at: http://www.statistics.gov.uk/cci/nugget.asp?id=2294

The findings suggest that many organisations have some BCM-related arrangements in place, such as remote working – but many managers do not think of them as such. It is encouraging that organisations have in place some methods for coping with disruption, but it is important for organisations to take a holistic approach to BCM, looking at their business to develop an overall strategy for disruption rather than relying on ad hoc responses (as discussed in Section 5.3).

4.3 Cyber and information security threats

As set out in the recent Strategic Defence and Security Review, the internet exposes organisations to a growing range of complex risks.[1] Managers were asked whether their organisation had suffered a range of IT related disruptions. Nearly a third of organisations' IT systems have been infected by a virus or malicious software in the past 12 months. Given that many viruses go undetected, the number to have been infected is likely to have been higher. In around one in ten organisations staff have lost confidential information and a similar number also suffered a significant attempt to break into their network.

Cyber threats	2011 %
Infection by a virus or other malicious software	32
Staff losing confidential information	12
Significant attempt to break into network	9
Staff leaking confidential information	7
Denial of service attack	2
Successful penetration by unauthorised outsider into your network	2

Table 3 Occurrence of cyber security threats over in the past 12 months

4.4 Influenza and employee illness

Employee illness is an occurrence that organisations deal with on a daily basis. However, epidemics or pandemics retain the potential to cause significant disruption on a much larger scale. Influenza represents the most likely and damaging source of a disruptive pandemic and in previous years this research has asked questions about preparations for swine flu and bird flu pandemics. This year the survey included questions about the impact of influenza in general terms. As Figure 8 shows, 57 per cent of organisations surveyed had only 5 per cent or fewer of their employees take time off because of influenza.
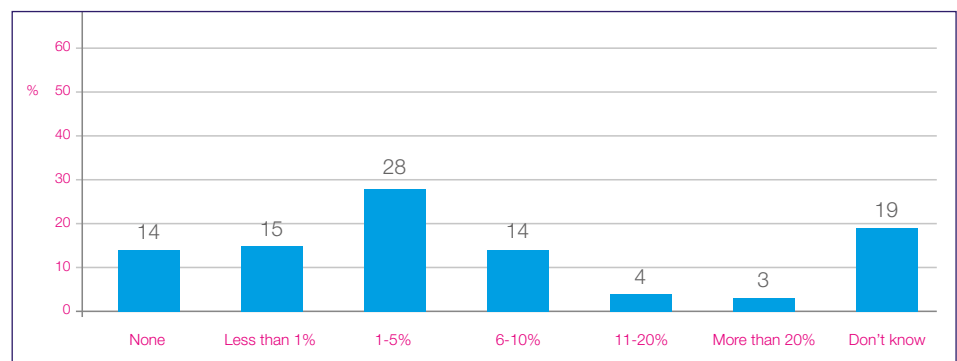

Figure 8 Percentage of employees who had time off due to influenza (over last 12 months)

1. The Strategic Defence and Security Review, HM Government (2010).
   www.number10.gov.uk/topstorynews/2010/10/strategic-defence-review-55906

As shown in Figure 9 below, only one in five managers agree that influenza poses a significant risk to their organisation. A clear majority (63 per cent) agree that the threat posed by swine flu in 2010 was overstated – though one in four say it led them to improve their business continuity arrangements, which is around 10 per cent higher than those revisiting BCM because of the Deepwater Horizon spill (as reported in Section 2). While many managers may feel that the dangers of swine flu were overstated, pandemic illness remains a real threat. Robust BCM arrangements which improve an organisation's resilience to influenza may also serve to mitigate the impact of staff shortages caused by a range of other risks such as travel disruptions due to bad weather.
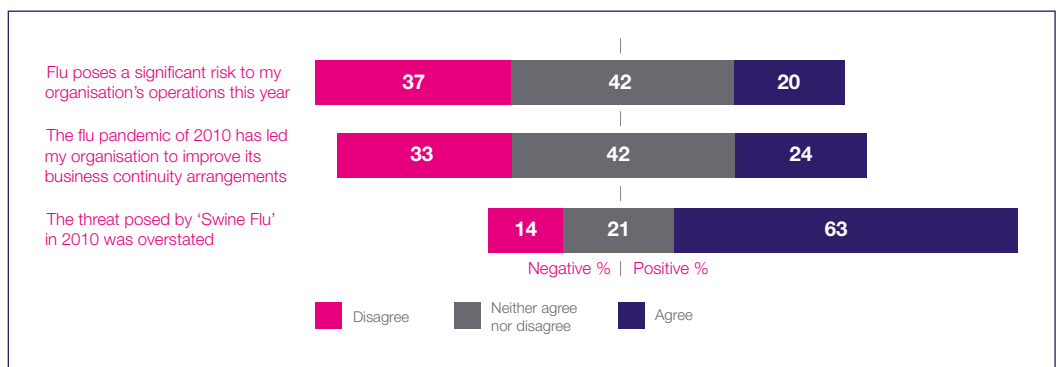

Figure 9 Attitudes to influenza

4.5 Remote working and alternative workplaces

As technology has advanced, organisational capacity for supporting remote working has increased. Although not applicable to every sort of job, remote working has become a central element of many organisations' BCM. Only 13 per cent of managers claim that their organisation has no alternative working arrangements in the event of a loss of access to the main workplace, whilst two thirds of organisations provide remote access to email systems and 57 per cent full remote access to IT systems (including access to files and software). Two out of five managers also have formal arrangements in place for alternative workplaces.

5. Developing the business case for BCM

5.1 The effectiveness of BCM

At its core, BCM should help an organisation cope with disruption, either enabling it to continue to deliver its critical services and products – or minimising the duration of interruptions and hastening a return to normal service. Respondents to the 2011 survey whose organisations have BCM are emphatic about the benefits. Where BCM has been activated in the last 12 months, 84 per cent agree that it effectively reduced disruption – up from 69 per cent last year. Furthermore, 77 per cent agree that the cost of developing BCM is justified by the benefit it brings their organisation.
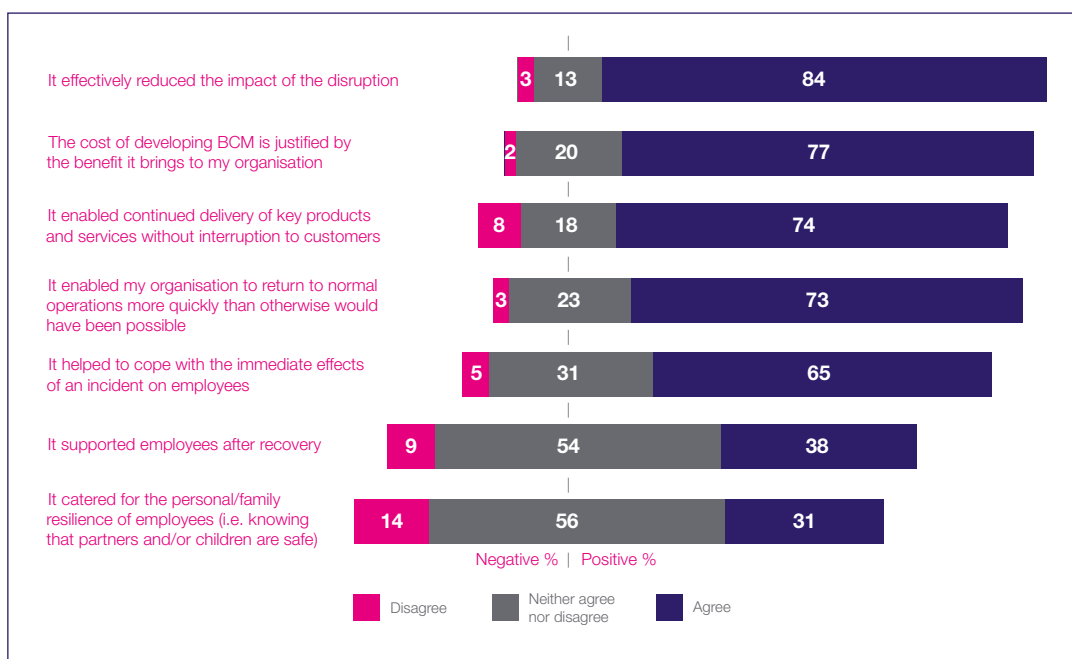

Figure 10 Managers' views on the effectiveness of BCM

Similarly, around three quarters of managers agree that it enabled their organisation to return to normal operations more quickly than otherwise would have been possible, while a similar number agree that it enabled their organisation to continue to deliver key products and services in the face of disruption.

Around two thirds of managers agree that their BCM helps employees cope with the immediate effects of an incident, but many fewer (38 per cent) agree that it helps employees post disruption. Similarly, only 31 per cent agree that their BCM caters for their employees' personal and family concerns, such as dealing with school closures or knowing loved ones are safe at a time of major disruption. This may represent a weak spot where improvements could be made in organisations' BCM. (To address this, BSI recently published PD 25111, the Human Aspects of BCM, setting out how organisations can address the human elements of business continuity.)

5.2 Benefits of having BCM

Anecdotal evidence has long suggested that organisations derive a number of additional benefits by implementing BCM besides the core gain in terms of preparedness for disruption. A new question sought to quantify these, as shown in Figure 11 below. Five benefits were cited by more than half of respondents. Among private sector managers specifically, 55 per cent also reported that it provides competitive advantage.
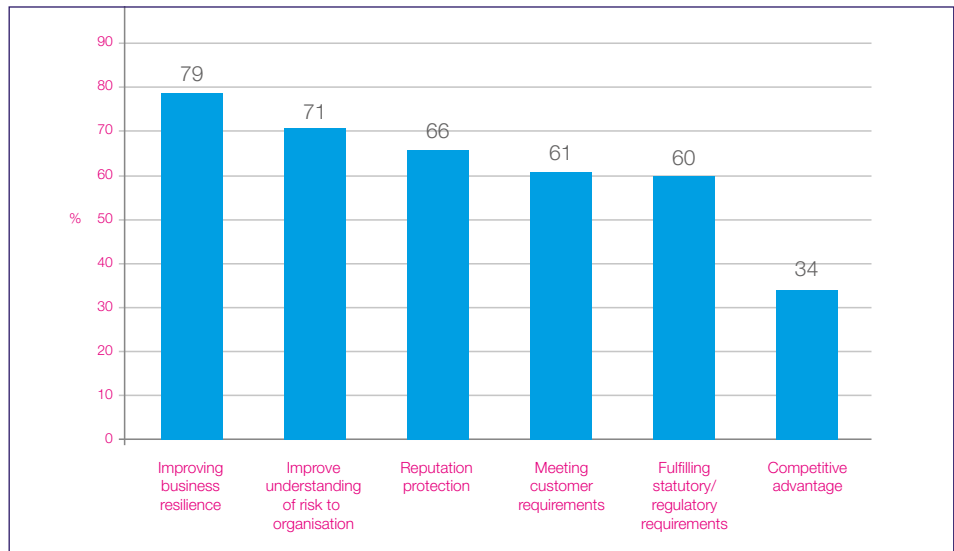
15

Figure 11 Perceived benefits of having BCM

5.3 Reasons for not implementing BCM

For the first time, 2011's survey asked "why not?" of those managers who report that their organisation does not have BCM[1]. Two in five suggest that their organisation does not suffer significant levels of disruption and a similar number say they deal with disruption on an ad hoc basis. Whilst certain organisations may well be exposed to more risk than others, it remains prudent to proactively develop BCM capability before a disruption, rather than risk being exposed when an unforeseen disruption occurs. It is encouraging that managers are generally not put off BCM by price or complexity.
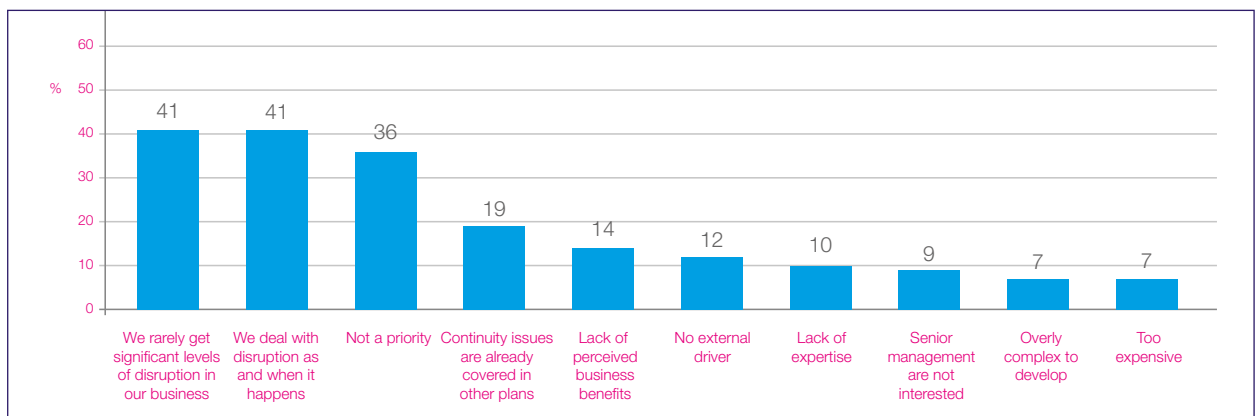

Figure 12 Reasons for not having BCM

5.4 External drivers of BCM

As well as the evident business benefits, many external drivers can influence an organisation's decision to implement BCM. Corporate governance is the biggest external driver with 42 per cent of managers reporting that it has acted as a catalyst for their organisation implementing or changing BCM. Customer demands are the next biggest driver, whilst for 23 per cent of organisations BCM provides competitive advantage.

1 Those who did not know whether their organisation had BCM were not included in this question.

Surprisingly, only 16 per cent of managers report that insurers drive adoption of BCM. In fact, their perceived influence in driving BCM has fallen in recent years, down from 17 per cent last year and 25 per cent in 2009.

There are large differences between economic sectors with 47 per cent of public sector organisations reporting central government as a key driver, compared to just 7 per cent in the private sector. Conversely, private sector organisations are more likely to report customers (40 per cent) and competitive advantage (34 per cent) as drivers than those in the public sector (24 per cent and 10 per cent, respectively).

Driver	2011 %	Driver	2011 %
Corporate governance	42	Regulators	19
Customers	33	Auditors	19
Competitive advantage	23	Insurers	16
Central government	22	Investors/finance providers	9
Legislation	21	Suppliers	7
Public sector procurement requirements	19	Not looked at BCM	15

Table 4 External Drivers of BCM

5.5 Supply chain issues

Effective BCM should not stop at the organisation's doorstep. Many organisations rely on outsource partners to deliver critical services and products and thus should ensure their BCM takes these into account. Yet 45 per cent of organisations with BCM do not require any supply chain partners to have their own plans, whilst 22 per cent are unsure whether they do or not. In 17 per cent of cases organisations require business critical suppliers to have a BCM in place. Five per cent require all their partners to have appropriate plans.

5.6 Components of effective BCM

BCM should provide a framework that builds organisational capability to respond to threats and safeguards the interests of key stakeholders, reputation, brand and value-adding activities. A new question in the 2011 sought to explore which components are included in organisations' BCM, as shown in Figure 13 below.

Large numbers described their plans as including strategies for maintaining the delivery of key products and services, IT back up exercises, arrangements for remote working and site emergency plans. Whilst appearing high, it is surprising that only 85 per cent say their BCM contains strategies for maintaining the delivery of key products and services – as this is the key function of BCM. This suggests that some organisations that appear to have BCM fall short of the good practice standards that might be expected.
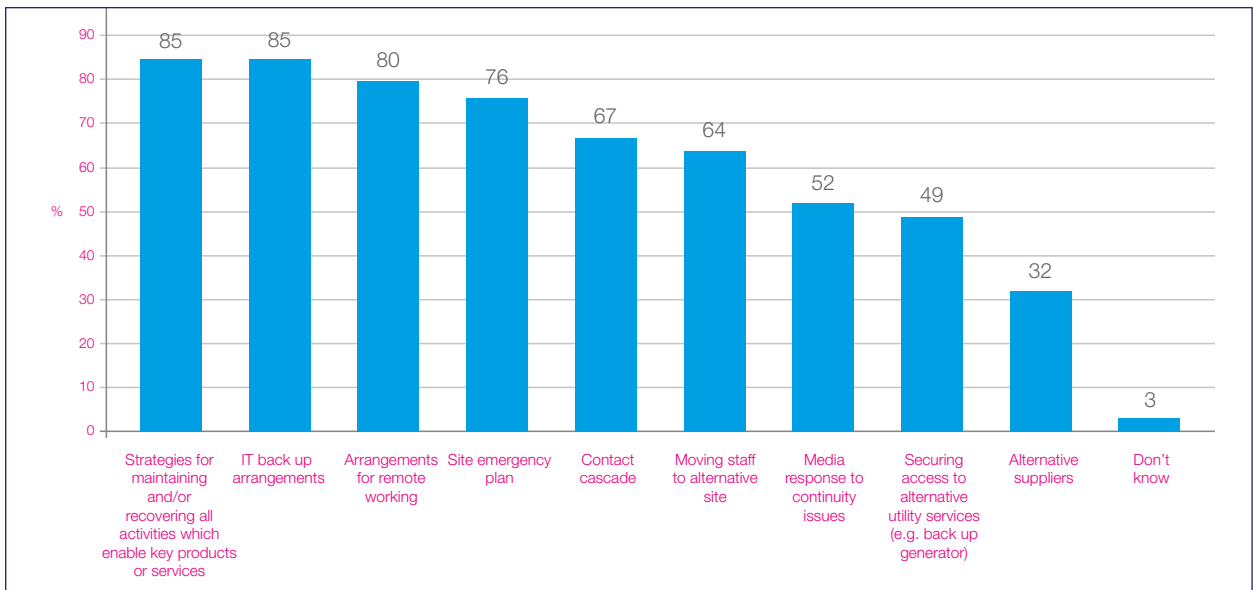
Figure 13 Common elements of BCM

5.7 Steps for developing BCM

At the core of developing BCM is an assessment of an organisation's business functions and the likely impacts that a disruption might have on them. Good practice dictates the need to conduct a formal business impact analysis, which two third of organisations undertook. More popular is a risk assessment exercise, which 83 per cent of organisations used, suggesting that many consider risk rather than the recommended approach of starting with an assessment of business impact.

Other common steps include identifying activities critical to service/product delivery, developing continuity strategies, creation of BCM policies and developing an internal communication plan. Only one in three organisations offer BCM related training to their non-specialist staff as part of BCM development (see also Section 5.9). One in five organisations used all the steps outlined in Figure 14 below.
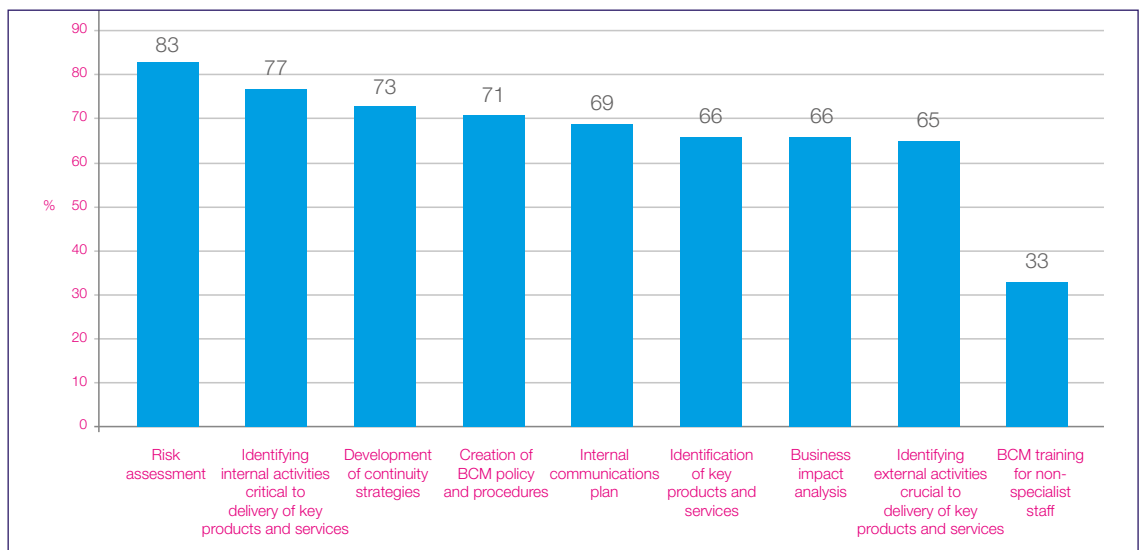

Figure 14 Commonly taken steps in developing BCM

There is a range of products and services that organisations can employ when developing BCM. Using networks to speak with someone who has previous experience is most common, used by 38 per cent, whilst a similar number used standards or guidance documents and 30 per cent online resources. Business impact analysis is also common. Specialist products and services, such as external training providers or software solutions, are less common.
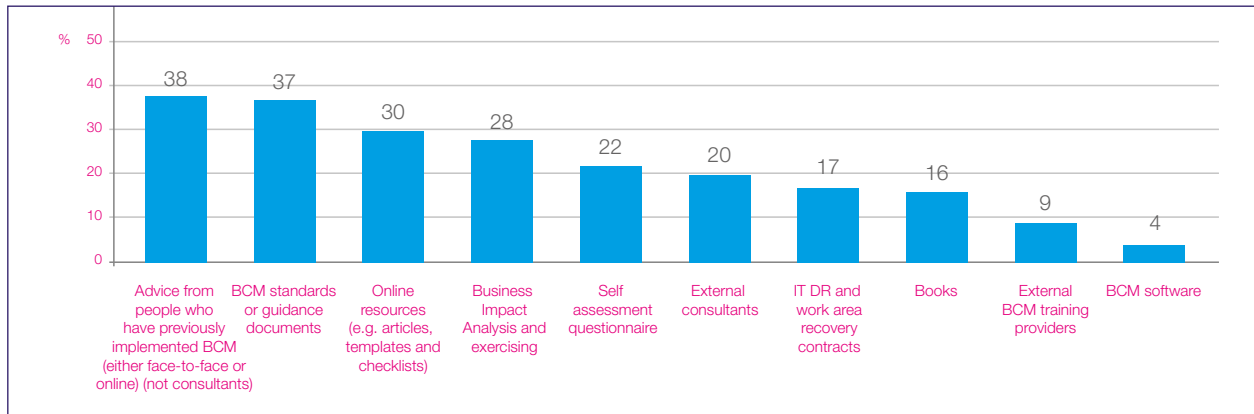

Figure 15 Products & services used when developing BCM

A further question looked at the sources of information used by managers for information on BCM. Internal sources are the most popular source (40 per cent), followed by professional bodies (32 per cent), central government (24 per cent) and then informal sources such as websites (18 per cent). Private sector SMEs, a group with relatively low levels of BCM and a key target group for policy makers, are more likely to use professional bodies (39 per cent) and informal sources (33 per cent) than other groups, suggesting tailored information should be distributed through these and similar channels. A list of potential resources is provided at the back of this report.

5.8 Exercising and evaluating BCM

Good BCM practice involves regularly exercising or rehearsing of BCM. This enables plans to be revised, refined and updated before weaknesses are exposed by a real disruption. Around a half of those organisations with BCM perform exercises once a year or more, with a quarter doing so at least twice a year. Around a quarter still fail to exercise their plans on a regular basis.

In 2010 the research showed that 70 per cent of those who had exercised their plans exposed shortcomings, demonstrating the value of such exercises. However, the scope and format of any exercise will greatly affect its potential for exposing weaknesses. Organisations should look to exercise their plans in full if they are to ensure they are robust in the face of disruption. As shown in Figure 16 below, currently only 29 per cent of organisations with BCM conduct a full emergency scenario exercise. (PD 25666, guidance on exercising and testing BCM, has recently been published by BSI to provide advice on how to improve this element of BCM.)
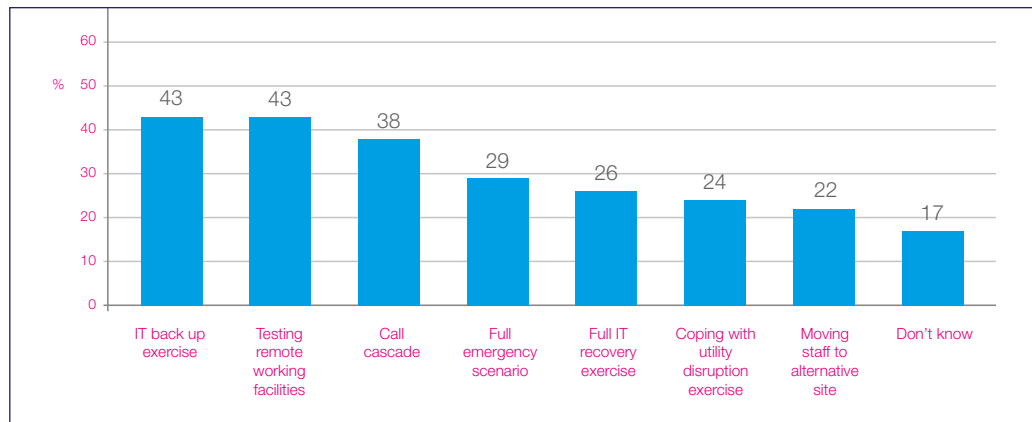
Figure 16 Format of BCM exercises

Evaluating BCM against established standards enables organisations to ensure that they meet good practice and are in a position to effectively cope with disruption. Many organisations, especially those in the public sector, are legally compelled to evaluate their plans against legislative and statutory requirements. The survey, once again, asked managers how their organisation evaluates its BCM. Two out of five did not know and one in five said their organisation does not evaluate BCM whilst around a third evaluate against legislative or regulatory requirements. One in ten evaluates their plans against BS 25999. When asked how BCM is audited, 43 per cent report self assessment with around a third using an internal audit and one in five employing a full scale external audit.

5.9 BCM training

Training employees to cope with disruption will help build an organisation's resilience. The survey revealed that 60 per cent of those organisations with BCM provide training to relevant staff, whilst 28 per cent do not, with the remaining 12 per cent of managers unsure. It is important that organisations train relevant staff, but as highlighted above only one in three organisations train non-specialist staff. There is a danger that organisations focus their training exclusively on BCM specialists when wider training is also needed to ensure staff know what to do at the time of disruption.

5.10 Responsibility for BCM

Throughout the research series, CMI has stressed the importance of senior management taking ultimate responsibility for BCM. Responsibility lies with either senior management, the board or the CEO/Managing Director in 69 per cent of cases. Twelve per cent have a dedicated BCM manager – the vast majority in the public sector.

BCM is a cross functional activity that covers all critical business services and products, and as such, should involve a variety of different departments and functions. When asked what functions are involved in their organisation's BCM the top three responses were: information technology (77 per cent), human resources (68 per cent) and facilities management (65 per cent). Public relations is involved relatively rarely (36 per cent) despite the assertion from managers that reputational risk is more damaging than financial loss.

6. Recommendations

Over three quarters of managers agree that the cost of developing BCM is justified by the benefits. Organisations not only stand to benefit from developing BCM, but they also have a responsibility to their stakeholders to protect the delivery of key products and services. It is strongly recommended that organisations develop proportionate and robust BCM.

Effective BCM

- The disruptions experienced by organisations may change from year to year, but the need to maintain delivery of critical services or products does not change. Organisations should take a holistic approach to BCM, focusing on the business impact, rather than on specific risks. Undertake a business impact analysis before a risk assessment.

- Organisations can change rapidly so review your BCM regularly, checking that it remains relevant to the organisation's current operations. This can support better understanding of the organisation as a whole.

- Use BCM based on a common framework (such as BS 25999) as part of a wider management strategy. It not only improves understanding of and resilience against business risks, but – as over half of private sector managers agree – it can give an organisation competitive advantage. Maximise these benefits by promoting them to internal and external stakeholders.

- Senior managers must take ultimate responsibility for the quality and robustness of their organisation's BCM. External communication may include statements in the directors' annual business review, helping to provide security to shareholders, employees, customers and other stakeholders.

- Develop a clearly defined approach for responding to the media at times of disruption. A majority of managers agree that reputational risk is a more significant threat than financial loss and as the Deepwater Horizon oil spill highlighted, the media response is critical during a major disruption. It may be just as important with local or trade publications as it is under the spotlight of the global media.

- It is strongly recommended that the effectiveness of BCM is tested through regular exercises. This will help to guard against plans becoming outdated as a result of changes in the organisation.

- Review which suppliers are critical to your operations and ask whether they have BCM. Recent high profile disruptions such as snow and volcanic ash affected many organisations' logistical operations.

Understanding changing threats

- This winter's extreme weather has been blamed for a 0.5% fall in GDP in the final quarter of 2010. Managers should develop BCM plans that would help them to deal with future bad weather.

- The interconnectedness of the UK's economy exposes organisations to an increasing and varied source of cyber and information security threats. Developing proactive strategies for dealing with the impact of such risks is an essential step for any organisations reliant on online networks and computer systems.

- More SMEs need to examine how they could use BCM. While some SME managers may argue that their size and agility may reduce exposure to disruption, a lack of resources also creates vulnerability in the event of a disruption. Professional bodies and others have a key role to play in promoting good practice guidance.

- Insurers should do more to promote BCM to their clients. Their influence could be critical in improving the uptake of BCM yet managers' perceptions are of declining influence on this agenda.

7. Help and advice

CMI Checklist on BCM and ManagementDirect service

CMI's Checklist on BCM is part of its popular range of over 200 Management Checklists, which help you develop your knowledge of and improve your practice in a management task, activity or skill. Free to CMI members, the Checklists are normally available for purchase via our website – but we have made the Checklist on BCM available for free download at **www.managers.org.uk/bcm2011**

Members of CMI also have access to the ManagementDirect portal – a unique information service that provides access to a range of management resources as well as informed researchers ready to answer your questions on key management issues. In addition, members are entitled to use one of the largest management libraries in the UK. Members can access these resources via **www.managers.org.uk/practical-support**

National Risk Register

The National Risk Register, published by the Cabinet Office, sets out the Government's assessment of the likelihood and potential impact of a range of different risks that may directly affect the UK. It is designed to increase awareness of the kinds of risks the UK faces and encourage individuals and organisations to think about their own preparedness. The register also includes details of what the Government and emergency services are doing to prepare for emergencies. It can be found at: **http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx**

BS 25999, PD 25666 and PD 25111

BSI Group is the publisher of BS 25999, a standard establishing the process, the process, principles and terminology of BCM. BS 25999 is published in two parts: Part 1 is a Code of Practice (2006) and Part 2 is a Specification (2007) giving the requirements for a Business Continuity Management System. Subsequent additional guidance has been published in the form of PD 25666, 'Guidance on exercising and testing for continuity and contingency programmes', and PD 25111, 'Guidance on human aspects of business continuity'. **www.bsigroup.com**

BCI Good Practice Guidelines

BCI's Good Practice Guidelines (GPG) draw upon the considerable academic, technical and practical experiences of the members of the Business Continuity Institute – senior practitioners who have developed and shaped the concept of Business Continuity internationally since its inception. The Guidelines are intended for use by practitioners, consultants, auditors and regulators with a working knowledge of the rationale for BCM and its basic principles. They cover the six phases of the BCM Lifecycle and link them to what are defined as 'Professional Practices', namely: Policy & Programme Management; Embedding BCM in the Organisation's Culture; Understanding the Organisation; Determining BCM Strategy; Developing and Implementing a BCM response; and Exercising, Maintaining and Reviewing. Find out more at **www.thebci.org/gpg.htm**

Appendix A – sector statistics

The table below outlines key findings from a range of industry sectors. It includes: the percentage in each sector with BCM; the most common drivers in that sector; the percentage of respondents that had not received any external requests for information on their BCM, which offers an indicator of how BCM is being driven; those that have full remote access to their IT systems; those who used a Business Impact Analysis when developing BCM; and, those who suffered major disruption as the result of this winter's weather.

Sector	With BCM %	Principal drivers	No external requests for BCM information %	Full remote access to IT systems %	Conducted Business Impact Analysis (organisations with BCM) %	Suffered major disruption from snow (Winter 2010/2011) %
Local Government	88	Corporate governance; Central Government; Legislation	10	60	73	37
Central Government	87	Central government; Corporate governance; Legislation	15	53	59	30
Finance, insurance	83	Regulators; Corporate governance; Regulators	25	73	70	25
Utilities	78	Regulators; Corporate governance; Insurers	11	78	71	47
Health and social care	64	Corporate governance; Regulators; Public sector procurement requirements	21	47	62	41
Transport and logistics	55	Corporate governance; Customers; Regulators	31	66	69	62
Education	49	Corporate governance; Customers; Central Government	37	63	66	38
Manufacturing and production	48	Customers; Competitive advantage; Corporate governance	24	62	69	35
Business Services	34	Customers; Corporate governance; Competitive advantage	57	48	80	37
Construction	26	Customers; Competitive advantage; Legislation	53	56	44	53

Appendix B – respondent profile 2011

Respondent profile	%
Managerial Level	
Director	27
Senior manager	32
Middle manager	29
Junior manager	12
Organisation Status	
Charity/not for profit	13
Public sector	36
Private sector	51
Region	
East of England	8
London	14
East Midlands	7
West Midlands	8
South East	18
South West	10
North East	4
North West	8
Yorkshire and the Humber	7
Northern Ireland	2
Scotland	8
Wales	3
Other	4
Number of employees	
1-10	19
11-50	12
51-250	15
251-1,000	15
1,000 or over	38

Base: 1053

Respondent profile	%
Sector	
Agriculture, forestry & fishing	0
Business services	4
Central Government	5
Construction	3
Consultancy	9
Creative/media	1
Defence	7
Education	13
Electricity, gas and water	2
Engineering	5
Finance & insurance	4
Fire and rescue	1
Health & social care	11
Hospitality, catering, leisure & tourism	2
Housing and real estate	3
IT	3
Justice/security	1
Legal & accounting services	1
Local Government	7
Manufacturing & production	8
Mining & extraction (inc. oil & gas)	1
Police	2
Sales/marketing/advertising	1
Telecommunications & post	2
Transport & logistics	3
Wholesale & retail	2

This report has been prepared in partnership with the following organisations:

The Civil Contingencies Secretariat

The Civil Contingencies Secretariat (CCS) sits within the Cabinet Office at the heart of central government. It works in partnership with government departments, the devolved administrations and with key stakeholders at national, regional and local levels across the public, private and voluntary sectors to enhance the UK's ability to prepare for, respond to and recover from emergencies. You can find out more, and contact CCS, via **www.cabinetoffice.gov.uk**

Business Continuity Institute

Based in Caversham, United Kingdom, the Business Continuity Institute (BCI) was established in 1994 to promote the art and science of business continuity management and to assist organisations in preparing for and surviving minor and large-scale man-made and natural disasters. The Institute enables members to obtain guidance and support from their fellow practitioners, and offers professional training and certification programmes to disseminate and validate the highest standards of competence and ethics. It has over 5,500 members in 90 countries active in an estimated 2,500 organisations in private, public and third sectors. For more information go to: **www.thebci.org**

Aon

Aon Corporation (NYSE:AON) is the leading global provider of risk management services, insurance and reinsurance brokerage, and human resources solutions and outsourcing. Through its more than 59,000 colleagues worldwide, Aon unites to deliver distinctive client value via innovative and effective risk management and workforce productivity solutions. Aon's industry-leading global resources and technical expertise are delivered locally in over 120 countries. Named the world's best broker by Euromoney magazine's 2008, 2009 and 2010 Insurance Survey, Aon also ranked highest on Business Insurance's listing of the world's insurance brokers based on commercial retail, wholesale, reinsurance and personal lines brokerage revenues in 2008 and 2009. A.M. Best deemed Aon the number one insurance broker based on revenues in 2007, 2008 and 2009, and Aon was voted best insurance intermediary 2007-2010, best reinsurance intermediary 2006-2010, best captives manager 2009-2010, and best employee benefits consulting firm 2007-2009 by the readers of Business Insurance. Visit **www.aon.com** for more information on Aon and **www.aon.com/manchesterunited** to learn about Aon's global partnership and shirt sponsorship with Manchester United. For more information on the Business Continuity practice at Aon, please contact either Vincent West on +44 (0)7889 406655/**vincent.west@aon.co.uk**, or Hugh Leighton on +44 (0)7885 417489/**hugh.leighton@aon.co.uk**

BSI Group

BSI Group is a global independent business services organisation that develops standards-based solutions to improve management practices and promote innovation. BSI can help businesses, governments and other organisations around the world to raise quality and performance in a sustainable and socially responsible way. From its origins as the world's first National Standards Body, BSI Group draws upon over 100 years' experience to work with 66,000 organisations in 147 countries from its 50 offices. Within Business Continuity, BSI Group is recognised for the publication of BS 25999 and as a leading certification and training provider in this field. In addition BSI has certified and trained organisations in BS 25999 in over 20 countries. To learn more, please visit **www.bsigroup.com**

Chartered Management Institute

The Chartered Management Institute is the only chartered professional body in the UK dedicated to promoting the highest standards of management and leadership excellence. CMI sets the standard that others follow.

As a membership organisation, CMI has been providing forward-thinking advice and support to individuals and businesses for more than 50 years, and continues to give managers and leaders, and the organisations they work in, the tools they need to improve their performance and make an impact. As well as equipping individuals with the skills, knowledge and experience to be excellent managers and leaders, CMI's products and services support the development of management and leadership excellence across both public and private sector organisations.

Through in-depth research and policy surveys of its 90,000 individual and 450 corporate members, CMI maintains its position as the premier authority on key management and leadership issues.

For more information please contact
the Policy and Research Department on:
Tel: **020 7421 2721**
Fax: **020 7497 0463**
Email: **research@managers.org.uk**
Website: **www.managers.org.uk**
or write to us at the address below.

Chartered Management Institute
2 Savoy Court, Strand,
London, WC2R 0EZ

Certificate No FS28404

INVESTOR
IN PEOPLE

4120 03/11