

# Horizon Scan 2013

## Survey Report



## Table of contents

	Forewords	1
1	Executive summary	3
	Key findings	
	Reviews and conclusions	
	Recommendations	
2	Introduction	7
3	Top threats in 2013	9
4	Trend analysis	13
5	Investment in business continuity	18
6	Comparison by primary activity	20
7	Comparison by geography	24
	<b>Annex</b>	
A	Analysis by geography and primary activity	29
B	Profile of survey respondents	39

## Foreword

### Lyndon Bird FBCI - Technical Director, BCI



Policy makers and business need to work together to ensure the benefits of cyber space are protected.

'The cyber threat is a critical issue that boards and policy makers have yet to get to grips with'. That is one of the startling conclusions from this ground-breaking global research project carried out by the Business Continuity Institute (BCI). The cyber threat is one of five key threats alongside data breach, unplanned IT and telecom outages, utility supplies and adverse weather revealed in this study.

Looking at underlying drivers of disruption, increasing supply chain complexity is a major challenge, and concern over a future pandemic is consistently affirmed across sectors and geographies. However, the stand-out trends of concern are all Internet related: the use of the Internet for malicious attacks, the influence of social media and the prevalence and high adoption of Internet-dependent services.

BCI members provide a unique perspective on the disruption faced by businesses and its consequences. And for the first time, long-term trends and shorter-term threats have been correlated in a way that helps businesses think about their short-term focus and longer-term capability development in order to become more resilient.

The research provides a clear call to action for policy makers and businesses to work together to ensure the benefits of cyber space for public services and industry alike are protected. The BCI is ready to play its part in supporting the required initiatives.

### About the BCI

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 8,000 members in more than 100 countries in an estimated 3,000 organisations in private, public and third sectors.

For more information visit [www.thebci.org](http://www.thebci.org)

## Foreword

### Howard Kerr - Chief Executive, BSI



Those that fail to act are at risk of sleep walking towards a reputational time bomb.

This latest report shows that businesses need to be more prepared than ever for every type of risk. Through careful management you can mitigate risk, increase recovery speeds and fulfil your regulatory and statutory obligations – helping you minimise the potential impact on your corporate reputation. For 20 years, BSI, together with industry experts, has pioneered international risk management standards including information security (ISO/IEC 27001) and business continuity management (ISO/IEC 22301).

This research also clearly shows that the digital age is continuing to bring new challenges to organisations around the world, with cyber attacks and data breaches worrying them the most. This is unsurprising given the increasing sophistication of these cyber attacks and the interconnectivity of technologies in the workplace.

Developing your cyber resilience must be an integral part of an organisation's wider business resilience strategy. Those that fail to act are at risk of sleep walking towards a reputational time bomb. By putting in place a framework based on risk standards, you will be able to identify, prioritise and manage threats more effectively.

### About BSI

BSI (British Standards Institution) is the business standards company that equips businesses with the necessary solutions to turn standards of best practice into habits of excellence. Formed in 1901, BSI was the world's first National Standards Body and a founding member of the International Organisation for Standardisation (ISO). Over a century later it continues to facilitate business improvement across the globe by helping its clients drive performance, manage risk and grow sustainably through the adoption of international management systems standards, many of which BSI originated. Renowned for its marks of excellence including the consumer recognized Kitemark®, BSI's influence spans multiple sectors including aerospace, construction, energy, engineering, finance, healthcare, IT and retail. With over 65,000 clients in 147 countries, BSI is an organisation whose standards inspire excellence across the globe.

For more information visit [www.bsigroup.com](http://www.bsigroup.com)

# 1

## Executive summary

Business continuity is about delivering resilient business performance, and protecting reputation.

The rationale behind the survey is to capture a consolidated view of near term threats that business continuity practitioners are concerned about based on their in-house analysis. This consolidated view is used by many to inform, and often confirm, planning assumptions.

Business continuity is about two things that are essential for a business to achieve its objectives – firstly, it is about delivering resilient business performance, and secondly it is about protecting reputation.

This report provides the results of the survey based on the overall survey sample of 730 organisations drawn from 62 countries around the world.

### Key findings

Unplanned IT and telecom outages is the leading cause of concern with 70% of respondents extremely concerned or concerned, followed by data breach (66%) and cyber attack (65%).

The top trends on the radar of business continuity professionals have a clear relationship to the top threats in 2013: the use of the Internet for malicious attacks is the number one trend of concern with the prevalence and high adoption of Internet services, such as cloud computing, in fifth position.

Supply chain disruption and increasing supply chain complexity feature prominently among threats and trends overall, but are top issues in sectors where adoption of business continuity has typically lagged behind other sectors, namely retail and manufacturing.

Climate change as an underlying trend does not feature prominently.

The influence of social media is the second most important trend for business continuity professionals to consider in their business continuity programmes with a score of 60%. The focus on this trend is truly boundary spanning in terms of maintaining this prominence across all sectors and geographies.

While adverse weather is a top five threat in the 2013 rankings, climate change as an underlying trend does not feature prominently, other than in Australia and among respondents working in the public administration sector.

New regulations and increased regulatory scrutiny takes third place with 56% in the list of trends and uncertainties, underscoring the business impact that uncertainty around and changes in regulation can bring, as well as the fact that many survey respondents work in regulated sectors.

Social and civil unrest features prominently as a threat in the Middle East and North Africa, where the threat of conflict in 2013 also reaches fifth position. However, this threat received a muted response overall.

The potential emergence of a global pandemic is under scrutiny by 41% of survey respondents, which is encouraging given the impact of the last pandemic in 2009, and respondents in the health and social sector, along with those in the UK and Canada, rate this uncertainty higher than the survey average.

77% of survey respondents confirmed that their organisation performed horizon scanning with 97% seeing the value of this information in their business continuity programmes. However, 32% of survey respondents stated they do not have access to trend analysis information. Even among those organisations where this is performed by colleagues in risk or strategy, 21% of business continuity practitioners did not have access.

Public administration and defence is expecting the most significant cuts and will see their ability to protect key services reduced.

Budgets for business continuity are robust overall, with 54% of respondents comfortable that the investment in 2013 will be appropriate for the needs of their programme, and 22% expected an increase to meet the needs of the programme. Above average growth can be found among organisations in Sub-Saharan Africa and the Middle East and North Africa. The sector which is expecting the most significant cuts is public administration and defence where 27%, almost double the survey average, will see their ability to protect key services reduced.

## Review and conclusions

The threats of most concern to business continuity practitioners are operational in nature, and oriented towards IT, telecommunications and the Internet. This is entirely consistent with and plays to the traditional strengths of business continuity practice.

This report does question whether such widespread concern over the cyber threat is justified based on the experience of actual disruption.

The high level of concern around the threat of a cyber attack in 2013 together with the extreme concern over the trend of using the Internet for malicious attacks is the most startling finding from this survey. Given the powerful economic forces driving the increasing adoption of Internet-dependent services, this concern can only grow. However, this report does question whether such widespread concern is justified based on the experience of actual disruption from cyber attacks, especially in relation to other threats. It may well be the case that the evidence and understanding of the threat is not there, hence high levels of concern are the natural result. Clearly, the cyber threat is a critical issue that boards and policy makers have yet to get to grips with.

Being prepared to anticipate and respond quickly to social media issues is a mandatory part of an effective business continuity programme.

The influence of social media is a trend that is dominating thinking in business continuity planning based on the results of this survey. While the survey did not seek to distinguish between social media's influence as a threat or opportunity, it can clearly serve to support both effective crisis communications as well as present a challenge in managing communications, especially where false information is being disseminated. It can equally be used as a channel to directly attack the brand reputation of a business. This challenge plays well to the strengths of business continuity with its focus on "time" - being prepared to anticipate and respond quickly to issues arising from social media sources is a mandatory part of an effective business continuity programme.

The survey results confirm the strong relationship between security and business continuity disciplines - both in the physical and virtual worlds. It is a surprise to see security incidents, such as vandalism, theft, fraud and protests reaching 6th position out of 29 threats but this confirms why many organisations see the merits of closer co-operation between business continuity and security professionals.

Supply chain disruption is a common concern for both executives and business continuity practitioners.

Supply chain disruption and increasing supply chain complexity feature strongly in the manufacturing and retail sectors as threats and trends of major concern. These sectors are the ones with comparatively low levels of business continuity adoption. So the results of this survey confirm that the value of business continuity to these sectors is going to be driven by perceived vulnerabilities and exposures in supply chains.

One observation from this year's results is the apparent lack of correlation between the threats that business continuity practitioners record and the typical threats published in top management risk surveys. Is this because top management does not appreciate the threats that actually cause disruption to business performance and reputation and therefore needs to be made aware of them? Or is it the business continuity community that needs to understand the risks that business executives care about and make them more prominent in their analysis and planning? That said, one of the common threats to executive and business continuity registers is often supply chain disruption. And perhaps the cyber threat is now on its way up executive agendas as well.

## Recommendations

The prominence of cyber threats as an area of extreme concern in the short term and the trend for higher dependency on Internet-based services and use of the Internet for malicious attacks makes this challenge one for boards and policy makers alike. We would advocate independent research into the actual threat and methods to deal with it to ensure the response is both effective and proportionate.

Horizon scanning as an activity needs to be part of a proactive business continuity programme. This activity needs to not only cover the common risk assessment through threat evaluation but also needs to consider the underlying and longer-term trends and uncertainties that may drive disruption. The good news is that this work is probably being conducted within organisations for different purposes within risk or strategy departments, so practitioners 'just' need to connect with their colleagues. Armed with this information, the business continuity practitioner will be able to ensure that there is a short-term focus coupled with a view on longer-term readiness requirements.



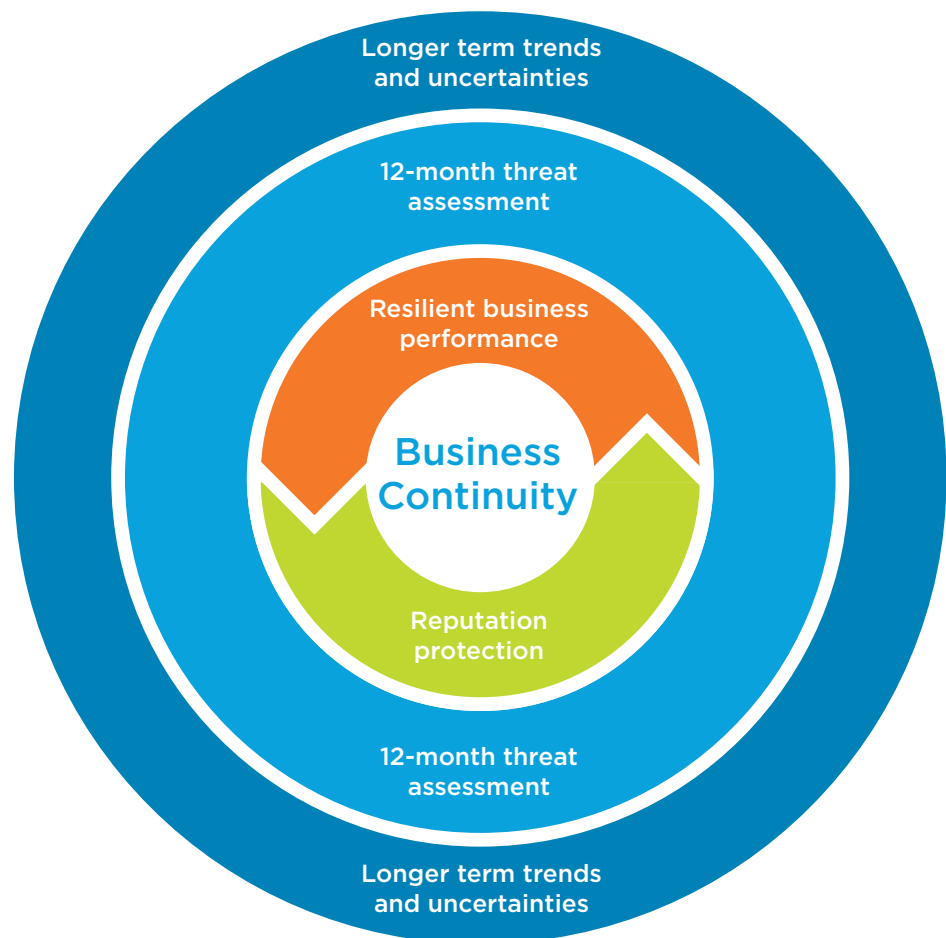
# 2

## Introduction

The rationale behind the survey was to capture a consolidated view of near term threats that business continuity practitioners are concerned about based on their in-house analysis. This consolidated view is used by many to inform, and often confirm, planning assumptions.

**Figure 2.1** sets out a simple construct to identify the relationship between business continuity and horizon scanning.

**Figure 2.1 - Horizon Scanning**



Business continuity is about two things that are essential for a business to achieve its objectives – firstly, it is about delivering resilient business performance, and secondly it is about protecting reputation. The threats that may cause impairment to business performance are well documented with some 29 sources offered in the survey. The new question raised by this year's survey is around the value of understanding longer-term or underlying trends and uncertainties, what these are, and how this insight is used to inform business continuity activities. For example, are current competencies and capacities appropriate for future challenges? Are planning assumptions related to symptoms or underlying causes? Another perspective on horizon scanning is that it enables business continuity practitioners to be pro-active within their organisations, especially where this analysis is not being performed.

The final part of the survey considers investment levels in business continuity in 2013. Are levels appropriate in light of the assessed threat horizon, are they increasing, or have they even been cut?

## About the survey

The significant jump in response levels indicates an increased interest in horizon scanning.

The online survey was open from November 19th until December 14th 2012. All BCI members received an email invitation to respond followed by a reminder email two weeks later. 730 validated responses were received drawn from 62 countries around the world. In the previous year's survey, 458 organisations responded to the survey, indicating a significant jump in interest in the topic.

In addition to this report providing the results based on the overall survey sample, it also provides a segmentation of the data by primary activity and geography to provide a more granular analysis. Overall, the results are very similar, however the data are analysed. This confirms a very common view held by business continuity professionals regardless of primary activity and geography when it comes to horizon scanning.

# 3

## Top threats in 2013

The top three threats rated by level of concern in this year's survey are:

- Unplanned IT and telecom outages  
(70% extremely concerned or concerned)
- Data breach  
(66% extremely concerned or concerned)
- Cyber attack  
(65% extremely concerned or concerned)

65% of respondents are concerned about a cyber attack in 2013.

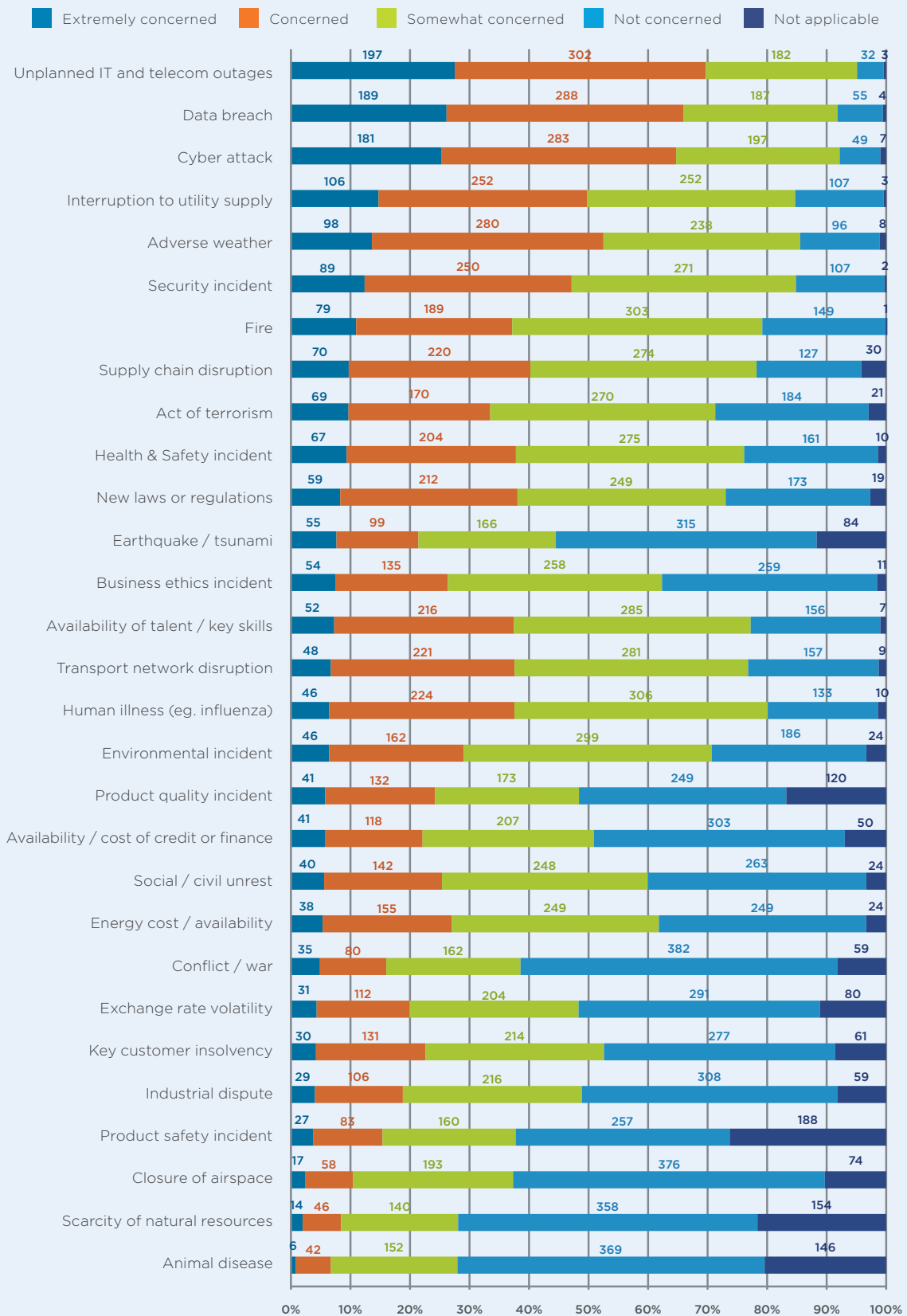
These three threats are ranked at some distance from the next cluster of threats, which include:

- Interruption to utility supply  
(50% extremely concerned or concerned)
- Security incident  
(47% extremely concerned or concerned)
- Adverse weather  
(53% extremely concerned or concerned)

Supply chain disruption holds its position as a top 10 threat in 8th place (40% extremely concerned or concerned).

**Figure 3.1** provides a break down against each of the 29 threats offered in the survey. They are ranked by level of concern, with extremely concerned followed by concerned dictating the final position in the table.

**Figure 3.1** - Based on your analysis, how concerned are you about the following threats to your organisation in 2013? (730 responses)



“Operating in the Middle East, I am particularly concerned about the potential for regional conflict.”

Survey respondent

“Our strategy is to bring ICT functions in-house to cut costs and reduce the risk.”

Survey respondent

“Due to the highly interconnected system in the financial industry, failure to meet the settlement timeline can pose severe liquidity risk not only to the clients but also to the banks”.

Survey respondent

In addition to the list of 29 threats, respondents offered some specific illustrations of the threats that concerned them. For example, under new laws and regulations, one respondent was concerned about government over-regulation and interference in markets, especially in food production and energy. Another was concerned that a change in government education strategy and funding methodology would have a major impact, for example a policy change regarding the desirability of maximising the number of young people going to university.

### Changes from last year's survey

There is a remarkable consistency in the ranking of threats between last year's 28 and the 29 in this year's survey. The new entrant was security incident, which offered security issues such as vandalism, theft, fraud and protests. It proved to be a significant new entrant in reaching 6th place. Among the top five, interruption to utility supply and adverse weather swapped places but otherwise there was no change among the top five.

Looking beyond the top 10 threats, the climbers are new laws and regulations, which moved from 15th to 11th position and product quality incident, which jumped from 25th position to 18th. Among those falling down the list were transport network disruption, energy cost or availability, and industrial disputes.

## FOCUS: Cyber threat

### **65% of respondents were concerned about a cyber attack in 2013, but is this fear justified by the evidence?**

Cyber incidents may well be under-reported but unless an incident is public and wide-scale this is always the case with disruption. This is one reason why the BCI conducts research such as Horizon Scan and its annual supply chain resilience survey to provide a mechanism to document levels and causes of disruption.

The operational consequences of cyber attacks have been tracked in a number of surveys run or supported by the BCI over the past three years. One consistent finding is that levels of cyber attacks are relatively low and are not causing significant disruption compared with other sources of disruption. There are specific sectors that are attractive targets along with their supply chains, but is the widespread concern justified?

In the 2012 Chartered Management Institute annual survey of disruption among its members, which is supported by the BCI, experience of a malicious cyber attack that caused disruption registered 6%, based on 1,021 respondents. In the previous year, the figure was 4% (based on 1,053 respondents). In contrast, 45% and 42% respectively were concerned about a cyber attack.

Looking at supply chain disruption, i.e., indirect cyber attack, the BCI's 2012 Supply Chain Resilience survey (based on 532 respondents), revealed that 16% experienced some or severe disruption as a result of cyber attack, but this was a long way down the list of events that had caused disruption. What is noteworthy, is that 41% of all recorded cyber attack incidents in this survey occurred within a single sector - financial services.

# 4

## Trend analysis

While threat evaluation through risk assessment is a common component of a business continuity programme, one of the survey's objectives was to understand the extent to which longer term analysis was conducted on trends and uncertainties.

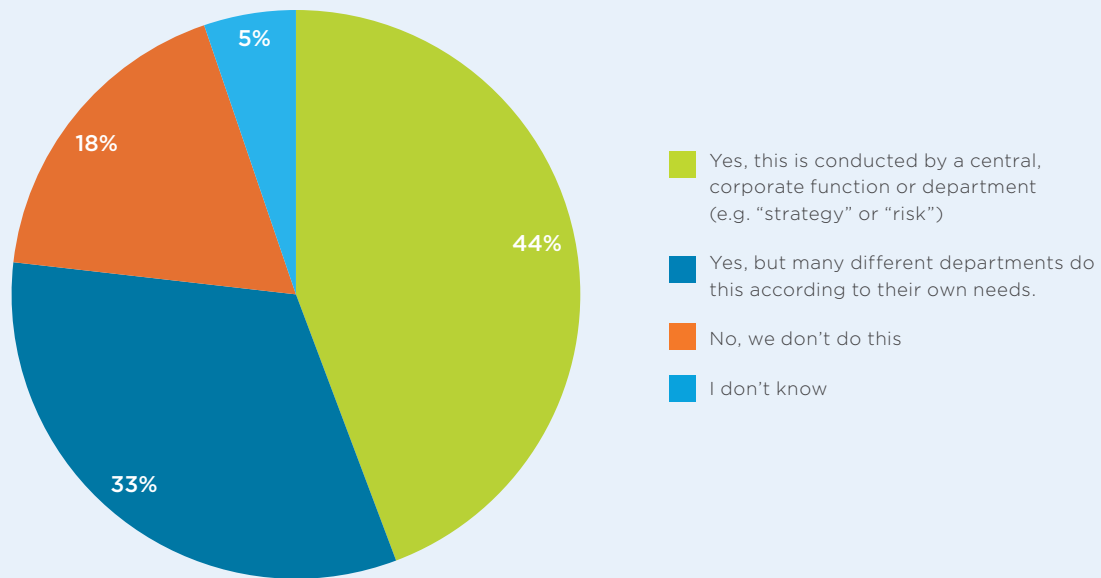
"More needs to be done in this area to make BC proactive rather than reactive"

Survey respondent

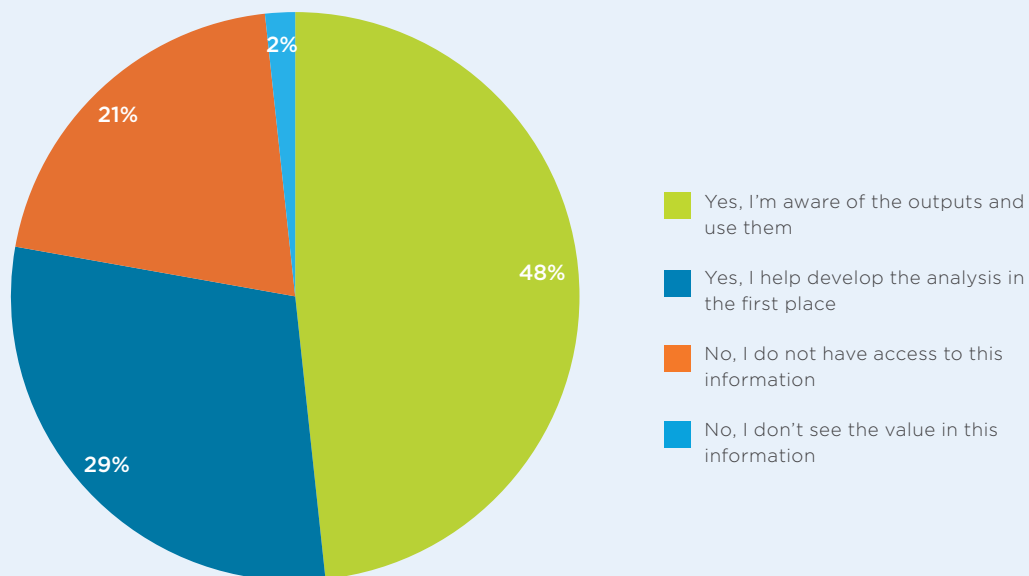
Overall, 77% of respondents confirmed that their organisation performed trend analysis. 18% stated their organisation did not do this as shown in **Figure 4.1**.

As a follow up question, the survey asked whether the survey participant drew upon the outputs of the trend analysis for their business continuity programme, for example as a basis for exercise scenarios or to consider areas of future capability. Overall 32% of survey respondents did not have access to this information. Considering only those who stated their organisation performed trend analysis and who responded to the question (532) still 21% did not have access to this information even though it exists. As silo-busters, business continuity professionals need to reach out to their colleagues to make use of the information. As shown in **Figure 4.2**, 48% are aware and use the outputs, while 30% are involved in developing the analysis in the first place. To complete the picture just 2% did not see the value of such information.

**Figure 4.1** - Does your organisation conduct longer-term trend analysis etc as part of its horizon scanning activity? (707 responses)



**Figure 4.2** - As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme (e.g. to develop scenarios or consider areas of future capability development)? (532 responses)



**Note:** Only those who stated their organisation performed trend analysis in the previous question are included here (i.e. 532 responses)



“While we try to consider a broad range of hazards and emerging risks, our company is organised so that responsibility for tracking many risks is assigned to departments other than business continuity management.”

Survey respondent

Another perspective on understanding the prevalence of trend analysis is to consider whether this activity is dependent on the size of the organisation. When using organisational size as a variable to understand approaches to trend analysis, there is a clear pattern, consistent with what one might expect.

Among those respondents working in organisations employing up to 500 staff, 28% do not undertake trend analysis as part of their horizon scanning. This figure falls to 18% in the segment covering employment of between 501 and 10,000 people. Among the very largest organisations, with more than 10,000 staff, only 9% do not perform such forms of analysis.

## Top trends

The survey asked, whether any of the 17 identified trends, emerging trends or uncertainties were on the responding organisation's radar for evaluation in terms of their business continuity implications. 695 responses were received to this question. The top five trends are listed below.

1. Use of the Internet for malicious attacks (cyber threat) - 71%
2. Influence of social media (reputation management, misinformation, crisis communications) - 60%
3. New regulations and increased regulatory scrutiny - 56%
4. Increasing supply chain complexity - 45%
5. Prevalence and high adoption of Internet-dependent services - 42%

The leading trend at 71% is the use of the Internet for malicious attacks. The strength of sentiment behind this trend is significant. Even when considered on a sector and geographical basis, its prominence is confirmed. This finding makes the need to understand the threat better even more important.

**Figure 4.3** - Which of the following trends or uncertainties are on your radar for evaluation in terms of their business continuity implications? (695 responses)



It may be surprising to see the influence of social media as a trend so high in the list but it indicates that the business continuity community has recognised the influence of social media as a significant change agent that along with its consequences - positive and negative - needs to be better understood.

New regulations and increased regulatory scrutiny is high, reflecting that many respondents operate in regulated sectors and, as identified earlier in the threats section, changes in policy can have significant business impacts.

Increasing supply chain complexity scores 45% and this trend is rated significantly higher in specific sectors such as manufacturing.

“The Cloud is a primary concern at the moment given data protection requirements and possibly not knowing where personal data is stored or if it is really secure.”

Survey respondent

Completing the top five is the prevalence and high adoption of Internet-dependent services, which offers “the cloud” as an example of this new dependency. As with supply chain optimisation, trends which are focused on taking cost out of operations are not “risk free” decisions for organisations, and the business continuity consequences need to be better understood.

Of the others, economic and social uncertainties generally scored less well, potentially indicating that such factors are too remote from operational concerns.

The potential emergence of a global pandemic, for example through poor drug management of antibiotics, maintains a steady position throughout thereby warranting active monitoring.

Given the focus on climate change and promotion of adaptation programmes, it is surprising to see this trend rated consistently low. Only respondents in public administration and defence (UK bias) scored this trend highly and on a geographical basis, respondents in Australia marked climate change highly as a consideration in their business continuity planning.

# 5

## Investment in Business Continuity in 2013

In this year's survey, we asked questions in respect of business continuity investments.

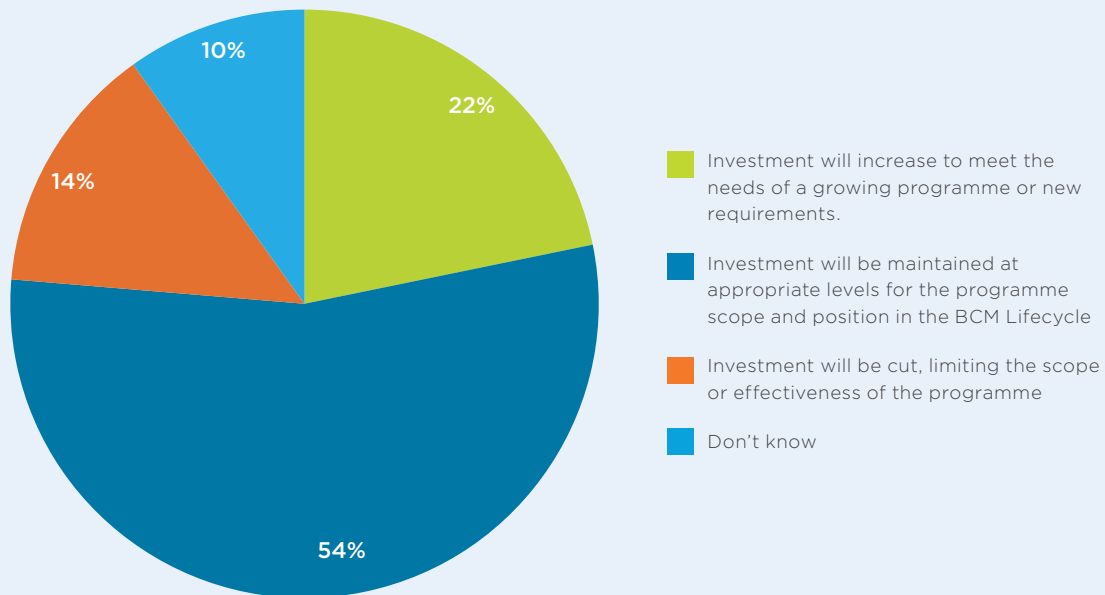
22% expect investments to rise in 2013 to meet the needs of a growing programme.

The first option was whether investment would increase to meet the needs of a growing programme or new requirements – 22% of 698 respondents confirmed this to be the expectation for 2013.

The second option asked whether investment would be maintained at appropriate levels for the programme scope and position in the BCM Lifecycle, 54% of respondents noted that this was the expected case. The final option was whether investment would be cut, thereby limiting the scope or effectiveness of the programme – 14% of the overall sample (96) stated that this would be the case. 10% did not know how investment levels in 2013 would compare to 2012 at the time of the survey. In the written comments, a further possible option was offered, which was that the current investment in business continuity was currently inadequate and this level of inadequacy was to continue into 2013.

Comparing the results with last year's survey, there is little change at the aggregate level. In Horizon Scan 2012, 25% expected an increase, 53% expected investment levels to be about the same, and 10% saw a decrease, with 12% not knowing. However, when analysed at a primary activity and geography level, some significant distinctions can be seen as described in Sections 6 and 7.

**Figure 5.1** - If you have a business continuity programme, how will investment levels in 2013 compare to the current year? (698 responses)



### Budget cuts

Of the 96 respondents who stated that their business continuity programme would face budget cuts in 2013, 22% came from the financial and insurance services sector and 23% came from the public administration and defence sector. In this sample, 42% did not have access to the trend analysis, well above the survey average.

"There is a fixed amount which will not be reduced but not increased either, even if we needed to."

Survey respondent

"Investment will be maintained as a below necessary rate."

Survey respondent

"Major work is underway with regards the vulnerability of assets to natural disaster."

Survey respondent

# 6

## Comparison by primary activity of the organisation

Annex A provides a full break-down of the sectors analysed in table form.

Eight sectors provided a sufficient sample for analysis:

1. Financial & insurance Services
2. Information and communication
3. Public administration & defence
4. Professional services
5. Manufacturing
6. Transport and storage
7. Health and social care
8. Retail

## Financial & insurance services

### Top threats:

- unplanned IT and telecom outages
- data breach
- cyber attack

This was the largest sub-segment with 223 responding organisations. 59% of respondents were based in the UK, USA, Australia and Canada. The top three threats were unplanned IT and telecom outages, data breach and cyber attack respectively. The overall ranking is similar to the aggregate survey results with two exceptions: new laws and regulations reaches 7th position in this sector compared with 11th overall, and availability/cost of credit or finance is in 10th place, compared with its 19th place in the overall sample.

In terms of access to trend analysis, 29% do not have access, while 26% are involved and 44% use it. The trends of most concern are use of the Internet for malicious attacks (79%) followed by new regulations and increased regulatory scrutiny (66%). The influence of social media is in third place at 60%.

In this sector, 26% see an increased budget in 2013, while 62% state it will remain the same and 10% foresee a cut.

## Information & communication

### Top threats:

- unplanned IT and telecom outages
- cyber attack
- data breach

There were 110 respondents in this sector, with 66% of respondents based in the UK, USA, Australia and Canada. The top three threats were the same as in financial and insurance services. In terms of trend analysis, 33% do not have access to trend analysis information, 36% are involved in the analysis, while 29% are not involved but use the information. In this sector a new trend joins the top three, in the form of prevalence and high adoption of Internet-dependent services, i.e. the Cloud.

In this sector 28% see an increased budget in 2013, while 50% state it will remain the same and 10% expect a reduction.

**Top threats:**

- unplanned IT and telecom outages
- cyber attack
- data breach

**Public administration & defence**

63% of the 103 respondents in this sector were based in the UK alone. Interestingly, the top three threats in 2013 by level of concern are the same as in the financial and insurance services sector. However, the trend analysis places social unrest in third position at 51% and climate change at 50%. These are the highest positions for these trends in any sector. In terms of budgets, 11% do see an increase, even in difficult economic times, while 44% believe that levels will remain the same and 27% see a cut.

**Professional services****Top threats:**

- data breach
- cyber attack
- unplanned IT and telecom outages

54% of the 89 respondents in this sector were active in organisations employing less than 250 people. While the top three threats are consistent with the overall survey sample, the threat to availability of talent and key skills figures prominently in 4th position. Business ethics incident reaches the top ten threats as well, as would be expected. In terms of trends, use of the Internet for malicious attacks dominates at 76%, followed closely by the influence of social media.

In this sector 26% stated their organisation does not perform trend analysis, while 29% do not have access to the information. 42% are aware of the information and use it, while 26% are actively involved in the analysis.

In terms of 2013 budgets, 68% expected investment to remain appropriate for the need while 13% expected an increase and 9% expected a cut.

**Manufacturing****Top threats:**

- supply chain disruption
- product quality incident
- product safety incident

The 39 respondents active in the manufacturing sector provide an interesting contrast to the overall survey sample. Supply chain disruption, product quality and product safety incidents take the top three positions. In terms of trend analysis, new regulations and increased regulatory scrutiny is a concern for 72%, slightly above increasing supply chain complexity with 69%. The use of the Internet for malicious attacks is a little adrift in joint third place at 53%. In terms of budgets, 11% expected an increased investment in business continuity, 53% felt investment levels would stay the same, while 21% expected a cut.



## Transport & storage

### Top threats:

- unplanned IT and telecom outages
- transport network disruption
- health and safety incident

There were 35 respondents who were active in this sector. The top three threats featured unplanned IT and telecom outages, transport network disruption and health and safety incident. Cyber attack and data breach reach 6th and 7th position in this sector. In terms of trend analysis, the major trend of concern was increasing supply chain complexity, selected by 64% of respondents. The use of the Internet for malicious attacks took second position with 55% and the influence of social media reached 49%. In terms of trend analysis, 33% do not have access to this information, 24% are directly involved while another 40% use it. In terms of budgets, 33% see an increase, 58% state budgets will stay the same and 6% expect to see a cut.

## Health & social care

### Top threats:

- unplanned IT and telecom outages
- data breach
- human illness

65% of the 31 respondents in the health and social sector are based in the UK. The top threat is unplanned IT and telecom outages followed by data breach and human illness. On the trend analysis question, the influence of social media leads with 63%, followed by the potential emergence of a global pandemic at 60% and increasing supply chain complexity in joint third position at 57%. Only 7% see an increase in budgets in 2013, while 23% expect a cut and 30% do not know.

## Retail

### Top threats:

- unplanned IT and telecom outages
- data breach
- supply chain disruption

One notable factor of the 20 respondents in the retail sector is that more than 70% of them are active in organisations with more than 10,000 staff. The top threats are led by unplanned IT and telecom outages followed by data breach. However supply chain disruption reaches third position in this sector. This finding is mirrored in the trend analysis, with increasing supply chain complexity being the primary concern for 70% of respondents in this sector. In terms of trend analysis, 35% do not have access, 25% are involved with 40% using the information. Budgets in this sector show great variation from the overall survey response at the two extremes with 40% seeing an increase, only 30% stating it will be the same, while 25% expect a cut. It should be noted that 18% did not know.



## Comparison by geography

Annex A provides a full break-down of the geographies analysed in table form.

Eight countries and regions provided a sufficient sample for comparison. In addition, a further 6 geographies have thumbnail assessments made in the Annex.

1. UK
2. USA
3. Continental Europe
4. Asia
5. Australia
6. Sub-Saharan Africa
7. Middle East & North Africa (MENA)
8. Canada

## UK

### Top threats:

- data breach
- unplanned IT and telecom outages
- cyber attack

291 respondents were based in the UK, providing a robust sub-segment for analysis. There were no surprises in the leading three threats in 2013: data breach, unplanned IT and telecom outages and cyber attack with adverse weather in 4th position. In terms of trends and uncertainties, 71% placed the use of the Internet for malicious attacks as their primary concern, followed by the influence of social media (60%) and new regulations or increased regulatory scrutiny (56%). Increasing supply chain complexity registered in 4th place with 50% of respondents, one of the highest levels in the overall survey.

In terms of trend analysis, only 18% of UK-based respondents stated that their organisation did not perform trend analysis. 34% do not have access to this information. 24% are involved in developing the analysis, while 39% use the information produced by others in their organisation.

In 2013, 14% expect to see an increase in business continuity spending to meet a growing programme, while 58% stated it will remain the same. 16% expect to see a cut.

## USA

### Top threats:

- unplanned IT and telecom outages
- data breach
- cyber attack

There were 95 respondents based in the USA. The top three threats in 2013 were given as unplanned IT and telecom outages, data breach and cyber attack with adverse weather in 4th place. In terms of trends and uncertainties, 80% placed the use of the Internet for malicious attacks as their primary concern, followed by the influence of social media and the prevalence and high adoption of Internet-dependent services (e.g. the Cloud).

Only 20% of US-based respondents stated that their organisation did not conduct trend analysis, however almost half (47%) do not have access to the information. 29% use the information provided while 22% are involved in developing the analysis.

In terms of investment levels in 2013, 31% see an increase, 48% expect levels to be appropriate, while 13% expect a cut.

## Continental Europe Cluster

### Top threats:

- cyber attack
- unplanned IT and telecom outages
- data breach

This group of European-based respondents totalled 100. The threat of cyber attack took first position among threats in 2013, the highest position of any geography. Unplanned IT and telecom outages and data breach completed the top three. In terms of trends and uncertainties, the leading three are the use of the Internet for malicious attacks (75%), followed by the influence of social media (61%) and new regulations or increased regulatory scrutiny (57%). Energy security and the transition to sustainable energy infrastructures registered in 7th place at 39%, much higher than its 12th position in the overall survey sample.

In terms of access to trend analysis information generated by their organisation, 24% do not have access. 32% are involved in the analysis, while 45% use the outputs in their BC planning.

Budgets in this geographical cluster are similar to the average, with 24% expecting an increase, 51% expecting it to be appropriate but not increasing and 17% expect a cut.

## Asian Cluster

### Top threats:

- data breach
- earthquake / tsunami
- unplanned IT and telecom outages

57 respondents were based in countries within the Asian cluster. It should be noted that 32% were active in the financial and insurance services sector and 30% in the professional services sector. Data breach was the leading threat for 2013, followed by earthquake/tsunami and unplanned IT and telecom outages. Cyber attack registered in 7th place only. However, on the trends analysis, the use of the Internet for malicious attacks top-scored with 70%, followed by new regulations and increased regulatory scrutiny (66%) and the influence of social media (52%). Interestingly, changing consumer attitudes and behaviour (e.g. towards personal data, customer experience) reached 4th position with 41%, its highest position in any country or region.

Respondents in this region tend to have access to trend analysis with only 18% stating they do not – almost half the level of the survey average. 38% are involved in the analysis. Only 14% of respondent organisations do not do trend analysis.

In terms of budgets only 7% see a cut in 2013, 63% expect investment levels to remain the same, while 23% see an increase.

## Australia

### Top threats:

- unplanned IT and telecom outages
- cyber attack
- adverse weather

For the 54 respondents based in Australia, the top three threats in 2013 were given as unplanned IT and telecom outages, cyber attack and adverse weather. In terms of trends and uncertainties, the use of the Internet for malicious attacks was cited by 58% of respondents with the influence of social media following on 56% and new regulations and increased regulatory scrutiny in third place. Climate change was in 4th position with 48% - the highest position of any country or region analysed.

In terms of access to trend analysis, 40% do not have access to the information with only 15% involved although 42% do use the information that is made available.

Investment in business continuity programmes will increase for 14%, stay the same for 53% and 22% will see a cut.

## Sub-Saharan Africa Cluster

### Top threats:

- unplanned IT and telecom outages
- cyber attack
- fire

39 respondents were based in countries in this region, with 54% active in the financial and insurance services sector. While unplanned IT or telecom outages and cyber attack featured as the leading threats in 2013, fire was placed in 3rd position. Looking further down the list, exchange rate volatility reached 8th place, significantly above its 23rd position in the overall survey rankings.

In terms of trends and uncertainties, new regulations or increased regulatory scrutiny scored 73% with the influence of social media in second place at 62% along with the use of the Internet for malicious attacks. The growing potential for social unrest is prominent in 4th position at 57% - much higher than in any other country or region. Entrenched organised crime also registers in joint 9th position compared with its 15th place in the overall survey.

Trend analysis according to the survey results is very much part of business as normal, only 5% of respondents stated that their organisation does not do trend analysis. Only 11% do not have access to the trend analysis information. 60% use the information generated, while 29% are involved in the analysis.

Investment levels for 2013 look very positive: Only 3% expect a cut, with 47% seeing an increase and 44% expecting investment to be the same.

## Middle East & North Africa Cluster

### Top threats:

- unplanned IT and telecom outages
- cyber attack
- fire

37 respondents were based in countries in this region. The list of top threats for 2013 are unplanned IT and telecom outages, followed by cyber attack and fire. The threat of conflict or war is in 5th position compared with 22nd position in the overall survey results with social or civil unrest in 6th position, compared with 20th position in the overall survey results. In terms of trends, the use of the Internet for malicious attacks leads the list on 64% followed by new regulations and increasing regulatory scrutiny with the influence of social media in 3rd at 49%. The growing potential for social unrest (e.g. through chronic unemployment, wealth inequalities or rising food costs) was chosen by 39% of respondents, reaching 4th position in the list of trends compared with 9th position in the overall survey.

40% of respondents in this region stated that their organisation does not perform trend analysis. A higher than average 42% do not have access to the information where it is produced.

In terms of budgets in 2013, this region is again seeing above average increases at 29%, with only 3% expecting a cut. 51% expect investment levels to be the same.

## Canada

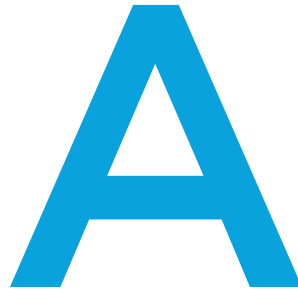
### Top threats:

- unplanned IT and telecom outages
- cyber attack
- data breach

The 30 respondents based in Canada followed the pattern of the overall survey on threats, but the threat of a business ethics incident was highly prominent in 5th place. In terms of trends and uncertainties, the potential emergence of a global pandemic was registered by 57% of respondents - the highest level in the survey. The lead trends were use of Internet for malicious attacks (79%), the influence of social media (71%) and new regulations or increased regulatory scrutiny (57%).

Among this group, 28% stated that their organisation did not perform trend analysis. Of those that do, 37% use the output without being involved, while 22% are involved, 37% do not have access to the information.

Budgets among the Canada based respondents follow the survey average with 25% seeing an increase in 2013, 54% seeing no change, while 14% expect a cut.



## Annex A - Analysis by geography and primary activity

**NOTE for all tables:** The Top 10 threats are ranked by the number stating “extremely concerned” followed by “concerned”.

### A1 Regional breakdown

**Figure A1.1 - Regional breakdown: UK (291 respondents)**

Top 10 threats		Top 10 trends/uncertainties	
1	Data breach	1	Use of the Internet for malicious attacks 71%
2	Unplanned IT and telecom outages	2	Influence of social media 60%
3	Cyber attack	3	New regulations and increased regulatory scrutiny 56%
4	Adverse weather	4	Increasing supply chain complexity 50%
5	Interruption to utility supply	5	Potential emergence of a global pandemic 47%
6	Supply chain disruption	6	Growing potential for social unrest 41%
7	Security incident	7	Prevalence and high adoption of Internet-dependent services 39%
8	Act of terrorism	8	Slow economic growth, fiscal imbalances, and their impact 38%
9	Fire	9	Climate change 36%
10	Human illness	10	Changing consumer attitudes and behaviour 31%

**Figure A1.2 - Regional breakdown: USA (95 respondents)**

<b>Top 10 threats</b>		<b>Top 10 trends/uncertainties</b>	
1	Unplanned IT and telecom outages	1	Use of the Internet for malicious attacks 80%
2	Data breach	2	Influence of social media 66%
3	Cyber attack	3	Prevalence and high adoption of Internet-dependent services 55%
4	Adverse weather	4	New regulations and increased regulatory scrutiny 53%
5	Interruption to utility supply	5	Increasing supply chain complexity 47%
6	Security incident	6	Potential emergence of a global pandemic 41%
7	New laws or regulations	7	Climate change 36%
8	Supply chain disruption	8	Slow economic growth, fiscal imbalances, and their impact 30%
9	Transport network disruption	9	Growing potential for social unrest 29%
10	Earthquake/tsunami	10	Enduring financial system weakness 28%

**Figure A1.3 - Regional breakdown: Australia (54 respondents)**

<b>Top 10 threats</b>		<b>Top 10 trends/uncertainties</b>	
1	Unplanned IT and telecom outages	1	Use of the Internet for malicious attacks 58%
2	Cyber attack	2	Influence of social media 56%
3	Adverse weather	3	New regulations and increased regulatory scrutiny 54%
4	Data breach	4	Climate change 48%
5	Fire	5	Prevalence and high adoption of Internet-dependent services 46%
6	Health and safety incident	6	Increasing supply chain complexity 46%
7	Act of terrorism	7	Changing consumer attitudes and behaviour 35%
8	Environmental incident	8	Potential emergence of a global pandemic 33%
9	Security incident	9	Slow economic growth, fiscal imbalances, and their impact 29%
10	Product quality incident	10	Enduring financial system weakness 21%



**Figure A1.4 - Regional breakdown: Canada (30 respondents)**

<b>Top 10 threats</b>		<b>Top 10 trends/uncertainties</b>	
1	Unplanned IT and telecom outages	1	Use of the Internet for malicious attacks 79%
2	Cyber attack	2	Increasing influence of social media 71%
3	Data breach	=3	New regulations and increased regulatory scrutiny 57%
4	Interruption to utility supply	=3	Potential emergence of a global pandemic 57%
5	Business ethics incident	5	Enduring financial system weakness 50%
6	Adverse weather	6	Climate change 46%
7	Availability of talent/key skills	=7	Growing potential for social unrest 39%
8	New laws or regulations	=7	Increasing supply chain complexity 39%
9	Security incident	=7	Slow economic growth, fiscal imbalances, and their impact 39%
10	Transport network disruption	10	Exchange rate volatility 36%

**Figure A1.5 - Regional breakdown: Continental Europe (100 respondents)**

<b>Top 10 threats</b>		<b>Top 10 trends/uncertainties</b>	
1	Cyber attack	1	Use of the Internet for malicious attacks 75%
2	Unplanned IT and telecom outages	2	Influence of social media 61%
3	Data breach	3	New regulations and increased regulatory scrutiny 57%
4	Interruption to utility supply	4	Prevalence and high adoption of Internet-dependent services 42%
5	Security incident	5	Increasing supply chain complexity 41%
6	Supply chain disruption	6	Potential emergence of a global pandemic 38%
7	Business ethics incident	7	Energy security and the transition to sustainable energy infrastructures 39%
8	Product quality incident	8	Slow economic growth, fiscal imbalances, and their impact 33%
9	New laws or regulations	9	Changing consumer attitudes and behaviour 32%
10	Fire	10	Climate change 29%

\* Europe (excluding the UK): this cluster covers 25 countries with 100 responses - Austria, Belgium, Bulgaria, Switzerland, Cyprus, Czech Republic, Germany, Denmark, Spain, Finland, France, Greece, Croatia, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, Sweden and the Slovak Republic.

**Figure A1.6 – Regional breakdown: Asia (57 respondents)**

<b>Top 10 threats</b>		<b>Top 10 trends/uncertainties</b>	
1	Data breach	1	Use of the Internet for malicious attacks 70%
2	Earthquake/Tsunami	2	New regulations and increased regulatory scrutiny 66%
3	Unplanned IT and telecom outages	3	Influence of social media 52%
4	Health and safety incident	4	Changing consumer attitudes and behaviour 41%
5	Security incident	5	Prevalence and high adoption of Internet-dependent services 39%
6	Interruption to utility supply	6	Increasing supply chain complexity 38%
7	Cyber attack	7	Potential emergence of a global pandemic 36%
8	Act of terrorism	8	Climate change 36%
9	Fire	9	Enduring financial system weakness 30%
10	Human illness	10	Growing potential for social unrest 30%

\* Asia: this cluster covers 11 countries with 57 responses: Bangladesh, China, Indonesia, India, Japan, Korea (Republic of), Malaysia, Philippines, Pakistan, Singapore and Taiwan.

**Figure A1.7 – Regional breakdown: Sub-Saharan Africa (39 respondents)**

<b>Top 10 threats</b>		<b>Top 10 trends/uncertainties</b>	
1	Unplanned IT and telecom outages	1	New regulations and increased regulatory scrutiny 73%
2	Cyber attack	2	Influence of social media 62%
3	Fire	=3	Use of the Internet for malicious attacks 62%
4	Interruption to utility supply	=3	Growing potential for social unrest 57%
5	Data breach	5	Prevalence and high adoption of Internet-dependent services 51%
6	Act of terrorism	6	Slow economic growth, fiscal imbalances, and their impact 51%
7	Security incident	7	Changing consumer attitudes and behaviour 46%
8	Exchange rate volatility	8	Climate change 43%
9	Energy cost / availability	=9	Entrenched organised crime 38%
10	Social/civil unrest	=9	Energy security and the transition to sustainable energy infrastructures 38%

\* Sub-Saharan Africa: this cluster covers 6 countries with 39 responses: Botswana, Kenya, Mauritius, Nigeria, South Africa and Zimbabwe.

**Figure A1.8 – Regional breakdown: Middle East & North Africa (37 respondents)**

<b>Top 10 threats</b>		<b>Top 10 trends/uncertainties</b>	
1	Unplanned IT and telecom outages	1	Use of the Internet for malicious attacks 64%
2	Cyber attack	2	New regulations and increased regulatory scrutiny 52%
3	Fire	3	Influence of social media 49%
4	Data breach	4	Growing potential for social unrest 39%
5	Conflict/War	5	Slow economic growth, fiscal imbalances, and their impact 36%
6	Social/civil unrest	6	Consumer attitudes and behaviour 36%
7	Act of terrorism	7	Prevalence and high adoption of Internet-dependent services 33%
8	Security incident	8	Exchange rate volatility 30%
9	Interruption to utility supply	9	Energy security and the transition to sustainable energy infrastructures 30%
10	Health and safety incident	10	Enduring financial system weakness 27%

\* Middle East and North Africa: this cluster covers 9 countries with 37 responses. UAE, Bahrain, Egypt, Israel, Jordan, Kuwait, Oman, Qatar, and Saudi Arabia.

## A2 Regional thumbnail Assessments

This information is provided for illustrative purposes only due to very small sample size.

**Figure A2.1 - Regional thumbnail assessment: Singapore (13 respondents)**

<b>Top threats</b>		<b>Top trends</b>	
1	Interruption to utility supply	1	Use of the Internet for malicious attacks 92%
2	Data breach	2	New regulations and increased regulatory scrutiny 67%
3	Unplanned IT and telecom outages	3	Changing consumer attitudes and behaviour 58%

**Figure A2.2 - Regional thumbnail assessment: China (15 respondents)**

<b>Top threats</b>		<b>Top trends</b>	
1	Data breach	1	New regulations and increased regulatory scrutiny 87%
2	Unplanned IT and telecom outages	2	Influence of social media 73%
3	Security incident	3	Use of the Internet for malicious attacks 67%

**Figure A2.3 - Regional thumbnail assessment: India (12 respondents)**

Top threats		Top trends	
1	Act of terrorism (55% extremely concerned)	1	Use of the Internet for malicious attacks 83%
2	Health and safety incident	2	New regulations and increased regulatory scrutiny 67%
3	Earthquake/tsunami	3	Enduring financial system weakness 58%

**Figure A2.4 - Regional thumbnail assessment: South Africa (20 respondents)**

Top threats		Top trends	
1	Cyber attack	1	New regulations and increased regulatory scrutiny 70%
2	Unplanned IT and telecom outages	=2	Influence of social media 60%
3	Data breach	=2	Use of the Internet for malicious attacks 60%
		=2	Prevalence and high adoption of Internet-dependent services 60%
		=2	Growing potential for social unrest 60%

**Figure A2.5 - Regional thumbnail assessment: New Zealand (12 respondents)**

Top threats		Top trends	
1	Unplanned IT and telecom outages	=1	Increasing supply chain complexity 73%
2	Earthquake/tsunami	=1	Influence of social media 73%
3	Health and safety incident	3	Use of the Internet for malicious attacks 64%

**Figure A2.6 - Regional thumbnail assessment: Latin America (15 respondents)**

Top threats		Top trends	
1	Earthquake/tsunami	1	Use of the Internet for malicious attacks 70%
2	Unplanned IT and telecom outages	2	Influence of social media 64%
3	Data breach	3	Energy security and the transition to sustainable energy infrastructures 50%

\* Latin America: this cluster covers 6 countries with 15 respondents: Argentina, Brazil, Chile, Colombia, Panama and Peru.

### A3 Primary organisational activity

**Figure A3.1** – Primary organisational activity: financial and insurance services  
(223 respondents)

Top 10 threats		Top 10 trends/uncertainties	
1	Unplanned IT and telecom outages	1	Use of the Internet for malicious attacks 79%
2	Data breach	2	New regulations and increased regulatory scrutiny 66%
3	Cyber attack	3	Influence of social media 60%
4	Interruption to utility supply	4	Potential emergence of a global pandemic 45%
5	Security incident	5	Increasing supply chain complexity 42%
6	Adverse weather	6	Prevalence and high adoption of Internet-dependent services 42%
7	New laws or regulations	7	Enduring financial system weakness 40%
8	Act of terrorism	8	Consumer attitudes and behaviours 35%
9	Fire	9	Climate change 34%
10	Availability/cost of credit or finance	10	Growing potential for social unrest 32%

**Figure A3.2** - Primary organisational activity: information and communication  
(110 respondents)

Top 10 threats		Top 10 trends/uncertainties	
1	Unplanned IT and telecom outages	1	Use of the Internet for malicious attacks 82%
2	Cyber attack	2	Prevalence and high adoption of Internet-dependent services 65%
3	Data breach	3	Influence of social media 58%
4	Security incident	4	New regulations and increased regulatory scrutiny 48%
5	Interruption to utility supply	5	Increasing supply chain complexity 40%
6	Fire	6	Slow economic growth, fiscal imbalances, and their impact 39%
7	Key customer insolvency	7	Potential emergence of a global pandemic 37%
8	Adverse weather	8	Consumer attitudes and behaviour 34%
9	Energy cost/availability	9	Energy security and the transition to sustainable energy infrastructures 33%
10	Health and safety incident	10	Growing potential for social unrest 32%

**Figure A3.3 - Primary organisational activity: public administration and defence (103 respondents)**

Top 10 threats		Top 10 trends/uncertainties	
1	Unplanned IT and telecom outages	1	Use of the Internet for malicious attacks 68%
2	Cyber attack	2	Influence of social media 56%
3	Data breach	3	Growing potential for social unrest 51%
4	Adverse weather	4	Climate change 50%
5	Act of terrorism	5	Potential emergence of a global pandemic 47%
6	Interruption to utility supply	6	New regulations and increased regulatory scrutiny 46%
7	Environmental incident	7	Increasing supply chain complexity 43%
8	Fire	8	Prevalence and high adoption of Internet-dependent services 38%
9	Availability of talent/key skills	9	Slow economic growth, fiscal imbalances, and their impact 37%
10	Health and safety incident	10	Enduring financial system weakness 20%

**Figure A3.4 - Primary organisational activity: professional services (89 respondents)**

Top 10 threats		Top 10 trends/uncertainties	
1	Data breach	1	Use of the Internet for malicious attacks 76%
2	Cyber attack	2	Influence of social media 72%
3	Unplanned IT and telecom outages	3	New regulations and increased regulatory scrutiny 59%
4	Availability of talent/key skills	4	Prevalence and high adoption of Internet-dependent services 50%
5	Interruption to utility supply	5	Slow economic growth, fiscal imbalances, and their impact 44%
6	Adverse weather	6	Potential emergence of a global pandemic 42%
7	Security incident	=7	Increasing supply chain complexity 38%
8	Business ethics incident	=7	Enduring financial system weakness 38%
9	Earthquake/tsunami	9	Changing consumer attitudes and behaviour 34%
10	Supply chain disruption	=10	Climate change 32%
		=10	Growing potential for social unrest 32%

**Figure A3.5 - Primary organisational activity: manufacturing (39 respondents)**

Top 10 threats		Top 10 trends/uncertainties	
1	Supply chain disruption	1	New regulations and increased regulatory scrutiny 72%
2	Product quality incident	2	Increasing supply chain complexity 69%
3	Product safety incident	=3	Use of the Internet for malicious attacks 53%
4	Health and safety incident	=3	Influence of social media 53%
5	Cyber attack	5	Global governance failures 31%
6	Data breach	6	Consumer attitudes and behaviour 31%
7	Unplanned IT and telecom outages	=7	Exchange rate volatility 28%
8	Scarcity of natural resources	=7	Potential emergence of a global pandemic 28%
9	Business ethics incident	=7	Energy security and the transition to sustainable energy infrastructures 28%
10	Interruption to utility supply	=7	Growing potential for social unrest 28%

**Figure A3.6 - Primary organisational activity: transport and storage (35 respondents)**

Top 10 threats		Top 10 trends/uncertainties	
1	Unplanned IT and telecom outages	1	Increasing supply chain complexity 64%
2	Transport network disruption	2	Use of the Internet for malicious attacks 55%
3	Health and safety incident	3	Influence of social media 49%
4	Adverse weather	4	Changing consumer attitudes and behaviour 46%
5	Supply chain disruption	5	Slow economic growth, fiscal imbalances, and their impact 42%
6	Cyber attack	6	New regulations and increased regulatory scrutiny 39%
7	Data breach	7	Growing potential for social unrest 33%
8	Closure of airspace	8	Climate change 27%
9	Act of terrorism	9	Potential emergence of a global pandemic 24%
10	Interruption to utility supply	10	Energy security and the transition to sustainable energy infrastructures 21%

**Figure A3.7 - Primary organisational activity: health and social care (31 respondents)**

Top 10 threats		Top 10 trends/uncertainties	
1	Unplanned IT and telecom outages	1	Influence of social media 63%
2	Data breach	2	Potential emergence of a global pandemic 60%
3	Human illness	=3	Increasing supply chain complexity 57%
4	Adverse weather	=3	Use of the Internet for malicious attacks 57%
5	Interruption to utility supply	5	New regulations or increased regulatory scrutiny 47%
6	Health and safety incident	6	Growing potential for social unrest 43%
7	Fire	7	Climate change 40%
8	Environmental incident	8	Slow economic growth, fiscal imbalances, and their impact 30%
9	Availability of talent / key skills	=9	Changing consumer attitudes and behaviour 23%
10	Cyber attack	=9	Energy security and the transition to sustainable energy infrastructures 23%

**Figure A3.8 - Primary organisational activity: retail (20 respondents)**

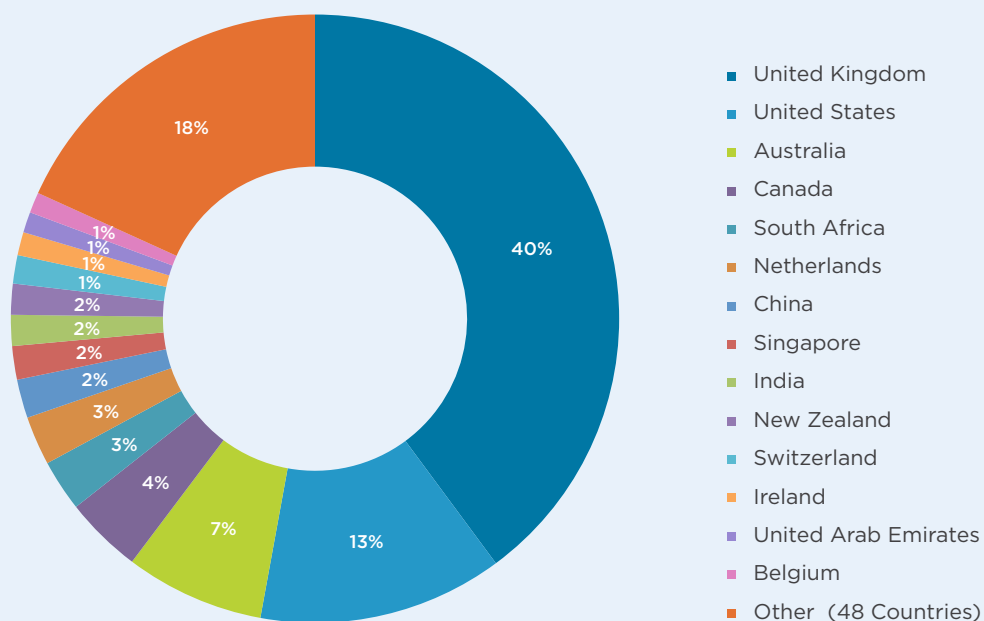
Top 10 threats		Top 10 trends/uncertainties	
1	Unplanned IT and telecom outages	1	Increasing supply chain complexity 70%
=2	Data breach	2	Influence of social media 65%
=2	Supply chain disruption	3	Use of the Internet for malicious attacks 65%
4	Adverse weather	4	New regulations and increased regulatory scrutiny 45%
5	Cyber attack	5	Prevalence and high adoption of Internet-dependent services 40%
6	Health and safety incident	=6	Global governance failures 35%
7	Interruption to utility supply	=6	Changing consumer attitudes and behaviour 35%
8	Fire	8	Globalisation (continuing) 30%
9	Business ethics incident	=9	Entrenched organised crime 25%
10	New laws or regulations	=9	Potential emergence of a global pandemic 25%

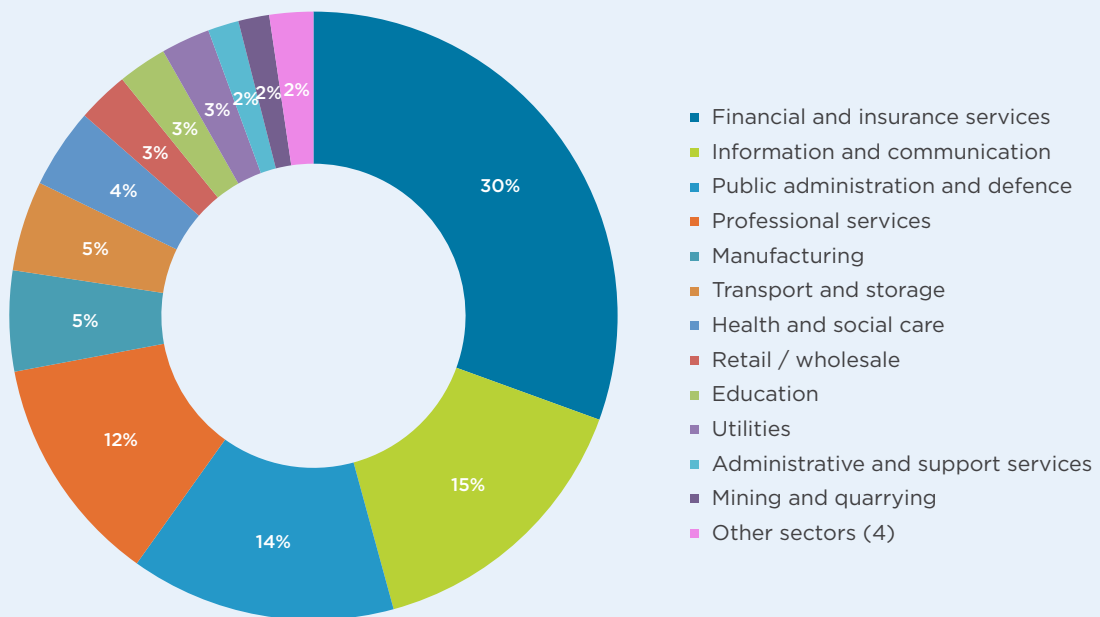
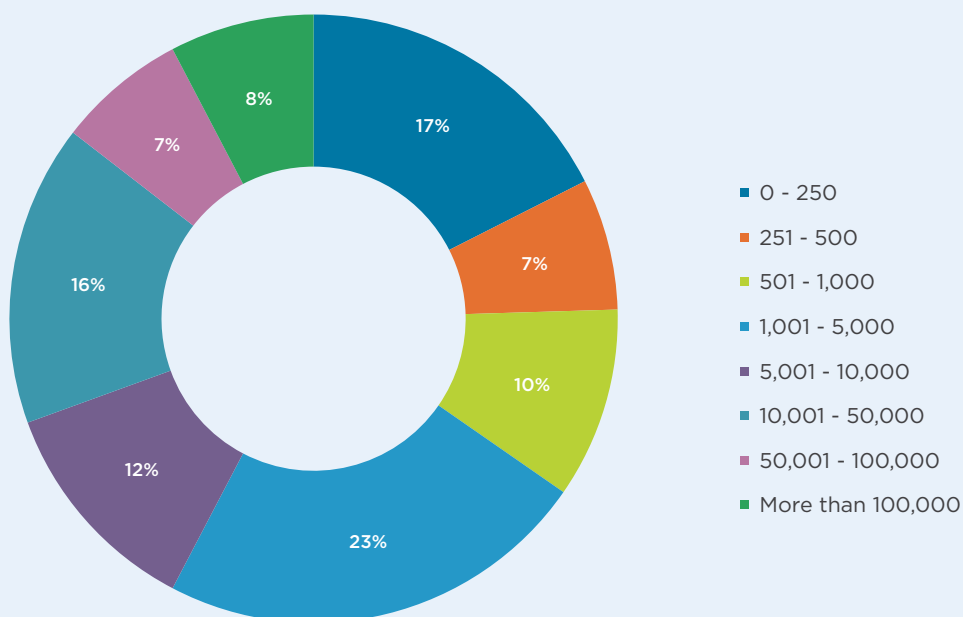


# B

## Annex B – Profile of survey respondents by country, primary activity and size of organisation

Figure B1 - Countries (730 respondents)



**Figure B2 - Primary activity (730 respondents)****Figure B3 - Size of organisation (730 respondents)**

## About the author



### **Lee Glendon CBCI**

Lee Glendon is Head of Research and Advocacy at the Business Continuity Institute. Lee is the author of the well-regarded Supply Chain Resilience series of research reports. He holds the Certificate of the BCI with merit, and is the inventor of BC24, the BCI's unique online incident simulation game, already played by some 2,000 corporate teams around the world. Prior to the BCI he worked in the telecoms sector for 10 years. He holds an honours degree in German and Business Studies from Warwick University.

**[lee.glendon@thebci.org](mailto:lee.glendon@thebci.org)**

**+44 (0) 118 947 8215**

This report provides a comprehensive view of the top threats faced by more than 700 organisations from 62 countries in 2013, along with an analysis of the underlying trends and uncertainties of concern that may cause future disruption.

© 2013 The Business Continuity Institute



**The Business Continuity Institute**

10 – 11 Southview Park,  
Marsack Street,  
Caversham, RG4 5AF, UK

**Tel:** +44 (0) 118 947 8215 **Email:** [research@thebci.org](mailto:research@thebci.org)

[www.thebci.org](http://www.thebci.org)