Business Continuity Institute

In association with... bsi.

Horizon Scan 2014

Survey Report

About the survey

The online survey was open from the 2nd December until the 27th December 2013 and was promoted to all Business Continuity Institute (BCI) members through direct email as well as the monthly newsletter. The survey was further promoted via a database of people with a known interest in BC and through BCI social media channels. 690 validated responses were received representing 82 countries.

Table of contents

Foreword

Lyndon Bird – Technical Director, BCI

Once again we find it is IT related threats that organizations are most concerned about with the level of this concern increasing considerably over the last year. Unplanned IT and telecom outages, data breaches and cyber attacks all make up the top three threats showing that as technology advances, even though it may provide us with opportunities we could not even imagine a few years ago, it also brings with it dangers that need to be addressed; dangers that could be through accidental means, and also dangers that materialise from more sinister intent.

The top three short term threats all being IT related is reflected in the longer term trends with the ***use of the internet for malicious attacks*** and ***the influence of social media*** making the top two. We often think of business continuity as an organization's ability to function despite the loss of certain aspects, and in this day and age, loss of reputation can be just as damaging as the loss of something more physical.

By having a wider spread of respondents than previous years, we are able to see more clearly the different threats that present themselves within different geographic locations. The survey certainly suggests that many people base their threat assessments on recent history and the experiences they have gone through. It also demonstrates that organizations must assess the threats that are relevant to them, whether those threats are due to the region or the industry they are in. All organizations face different challenges so must never lose focus on those specific to them.

With budgets tight and investment in BC programmes remaining the same in all but a few organizations, it is even more important that organizations use what money they have more wisely and only invest in BC plans that are relevant to them.

This piece of research has greater significance this year as we celebrate the 20th anniversary of the BCI. As part of our commemorations we have launched the 20/20 Mission, a campaign that is all about looking to the future and facing the new challenges this future will bring.

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 organizations in preparing for and surviving minor and largescale 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 organizations in private, public and third sectors.

For more information visit www.thebci.org

Foreword

Howard Kerr – Chief Executive, BSI

At a time when business is more vulnerable to a myriad of risks – from globalisation and interdependency in the supply chain to more localised threats – this latest report shows that businesses need to be more prepared than ever. Managing risks and the continuity of your operations is critical to the reputation, survival and growth of your business.

This research reveals that changing technology, the increasing value of data and new legislation is continuing to bring challenges to organizations around the world, with ***unplanned IT and telecommunication outages*** as well as the risk of ***data breaches and cyber attack*** worrying business the most. This is unsurprising, given the risks associated with the growing complexity and reliance on technology over the past decade. What is surprising is that a fifth of organizations admit to operating and planning in the dark, with little or no visibility of real time data. You cannot protect against something you can't see.

Developing the resilience of networks, services and business critical information must be an integral part of an organization's wider business resilience strategy. At a time when changing climatic, social, political and economic situations are forcing organizations to be nimble in adapting to novel threats, it is essential to learn from others experience and best practice. By putting in place a framework based on risk standards, you will be able to identify, prioritise and manage the range of threats to your business more effectively and keep your stakeholders reassured.

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 Organization for Standardization (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 BSI Kitemark™, BSI's influence spans multiple sectors including aerospace, construction, energy, engineering, finance, healthcare, IT and retail. With over 70,000 clients in 150 countries, BSI is an organization whose standards inspire excellence across the globe.

To learn more, please visit www.bsigroup.com

1. Executive summary

Key findings

The top three threats for organizations remain the same as previous years. ***Unplanned IT and telecom outages*** is considered the greatest threat with 77% of respondents extremely concerned or concerned, followed by ***data breach*** (73%) and ***cyber attack*** (73%). The percentage of people showing concern for all three of these threats has increased considerably during the year.

There was some movement within the top ten as ***cyber attack*** (3->2), ***adverse weather*** (5->4) and ***fire*** (7->6) and ***health and safety incident*** (10->8) all moved up places. Going the other way, ***data breach*** (2->3), interruption to utility supply (4->5) and ***security incident*** (6->7) all moved down. ***New laws or regulations*** entered the top ten in tenth place (11->10) while exiting the top ten with the biggest change from the previous year was ***supply chain disruption*** (8->16).

There were some geographic variations that stood out. ***Earthquake/tsunami*** is one of those as it was considered a threat by respondents from both Japan (83%) and New Zealand (71%) and this is clearly a result of recent experience. Respondents from Japan also considered ***human illness*** (61%) as a threat and this can again be attributed to the sheer scale of the natural disaster the country suffered from in 2011 and the aftermath of that. ***Interruption to utility supplies*** was considered the number one threat by respondents from Sub Saharan Africa (70%).

For primary activity, ***security incident*** (57%) was considered a top three threat to those respondents whose primary activity was education. Similarly ***health and safety incident*** (68%) and ***human illness*** (68%) both appear as top three threats on only one occasion and these were with respondents from within the health and social care sector. ***Supply chain disruption*** (60%) and ***product quality incident*** (60%) both appear as a major threat for those within the manufacturing industry and ***adverse weather*** (69%) is deemed a threat for those working in ***public administration and defence***.

Similarly with trends, those which are on the radar of business continuity professionals are those linked to these top three threats. The use of the ***internet for malicious attacks*** is again number one with 73% of respondents expressing concern followed by the ***influence of social media*** (63%) in second place and ***high adoption of internet dependent services*** (48%) in fourth place. Sandwiched between these two is ***new regulations and increased regulatory scrutiny*** in third place (55%).

Overall, 71% of respondents confirmed that their organization did perform trend analysis while 22% stated their organization did not. However, of those who stated their organization did perform a trend analysis, an astonishing 20% still did not have access to this information even though it exists, 53% are aware and use the outputs, 26% were involved in developing the analysis in the first place and only 1% failed to see the value of such information.

Despite the increased concern of the threats, the level of investment in BC programmes is being maintained at current levels for the vast majority of organizations. Only 18% are increasing their budget and 11% are actually decreasing it. This suggests that for the majority of organizations, little has changed in the perceived threat levels to justify any change in expenditure.

It was noted that less than a half of respondents (44%) currently use ISO 22301 as a framework for their business continuity management programme although about a quarter (24%) claimed they were planning to adopt it as a framework during 2014.

Review and conclusions

The survey results clearly show that the threats of greatest concern to business continuity professionals are those related to IT and communications, the two areas that are often considered the cornerstone of the and where it originated from.

The fall of ***supply chain disruption*** as a perceived major threat comes as a surprise given the nature of the potential disruption caused, an area of concern demonstrated in the BCI's Annual Supply Chain Resilience Report. This fall was also a surprise given that ***increasing supply chain complexity*** featured so highly as a trend (45%).

The fact that there is a certain amount of variation between businesses in different sectors and more so between organization in different geographic locations highlights the importance of conducting horizon scans that are specific to the activity/location of the organization. Organizations all face different threats so the horizon scanning process is crucial to establish what these threats are before considering the impact of them and how this impact can be reduced.

It is also clear from the examples of Japan, New Zealand and India that perception of threats is almost always dependent upon recent history. Perhaps this is more a case of hindsight scanning than horizon scanning but it demonstrates that experience plays a key role in determining threats.

With a fifth of respondents stating their organization did not conduct a trend analysis, and a fifth of those who did conduct such an analysis saying that they don't have access to the output, many organizations are being left blind as to threats they face and how they would deal with them.

Recommendations

The prominence of the IT related threat, whether it is by way of accident or more malicious intent, is something that business continuity professionals and organizations need to take on board. Organizations need to invest in the development of technologies that can help counter these threats and, perhaps just as importantly, they need to find ways of adapting their organization so they can still function should the threat materialise. This may not be so easy given that investment is not increasing for the majority of organizations, so perhaps those in the industry need to put greater emphasis on what the immediate return on investment of a business continuity programme is.

2. Introduction

The annual BCI Horizon Scan survey is designed to assess the short term threats that businesses continuity practitioners are most concerned about. This is based on in-house analysis of data provided by those practitioners.

The survey also sought to establish whether organizations are actively horizon scanning and what access BC professionals have to this information once the horizon scanning process has been completed.

It is by developing a better understanding of these threats that business continuity practitioners can learn how to protect their organizations against them should they materialise, thus increasing the likelihood of the organization functioning as normal and reducing the potential for operational and reputational damage.

The survey considers investment levels in business continuity in 2014. Are levels appropriate in light of the assessed threat horizon, are they increasing, or have they even been cut?

The final part of the survey looked at the adoption of ISO 22301 and whether organizations were starting to use this relatively new standard as a framework for the BC management programme.

As Figure 2.1 shows, one third of respondents were based in the United Kingdom and this reflects the high BCI membership in this country.

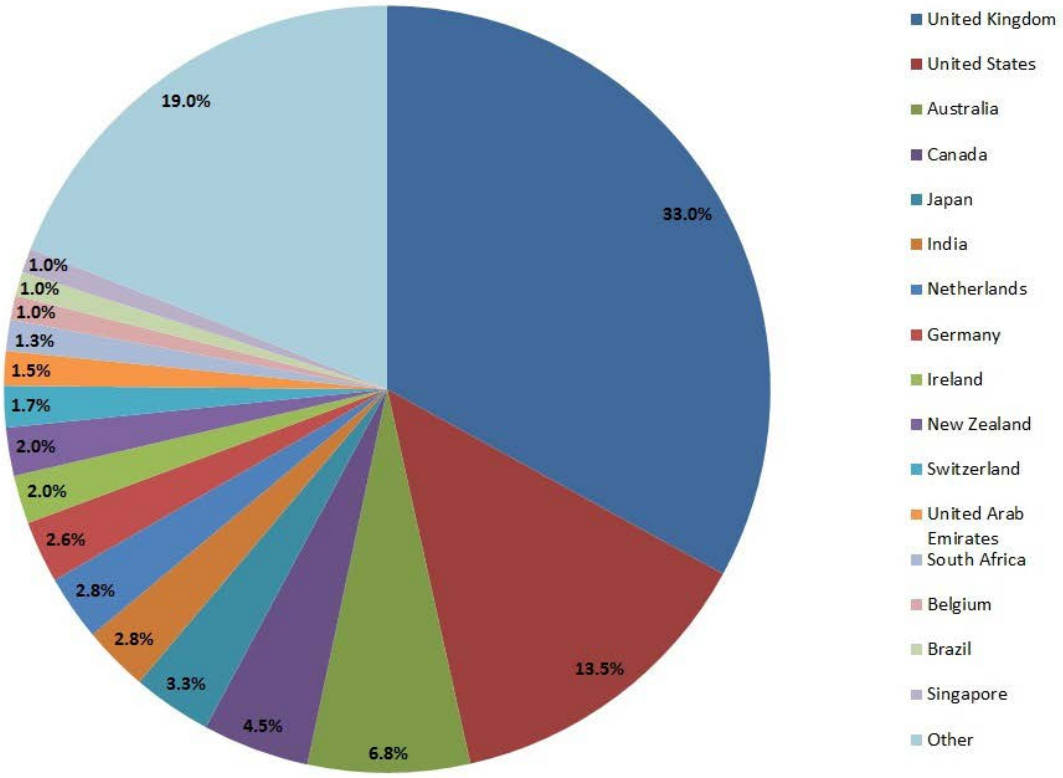

Figure 2.1: Respondent breakdown by geography

Figure 2.2 shows the breakdown of respondents by the primary activity of their organization. People working in the ***financial and insurance services sector*** featured highest with over a quarter of respondents employed in this sector. This was followed by people working for organizations in the ***information and communication and professional services*** sectors, both with around 14%.

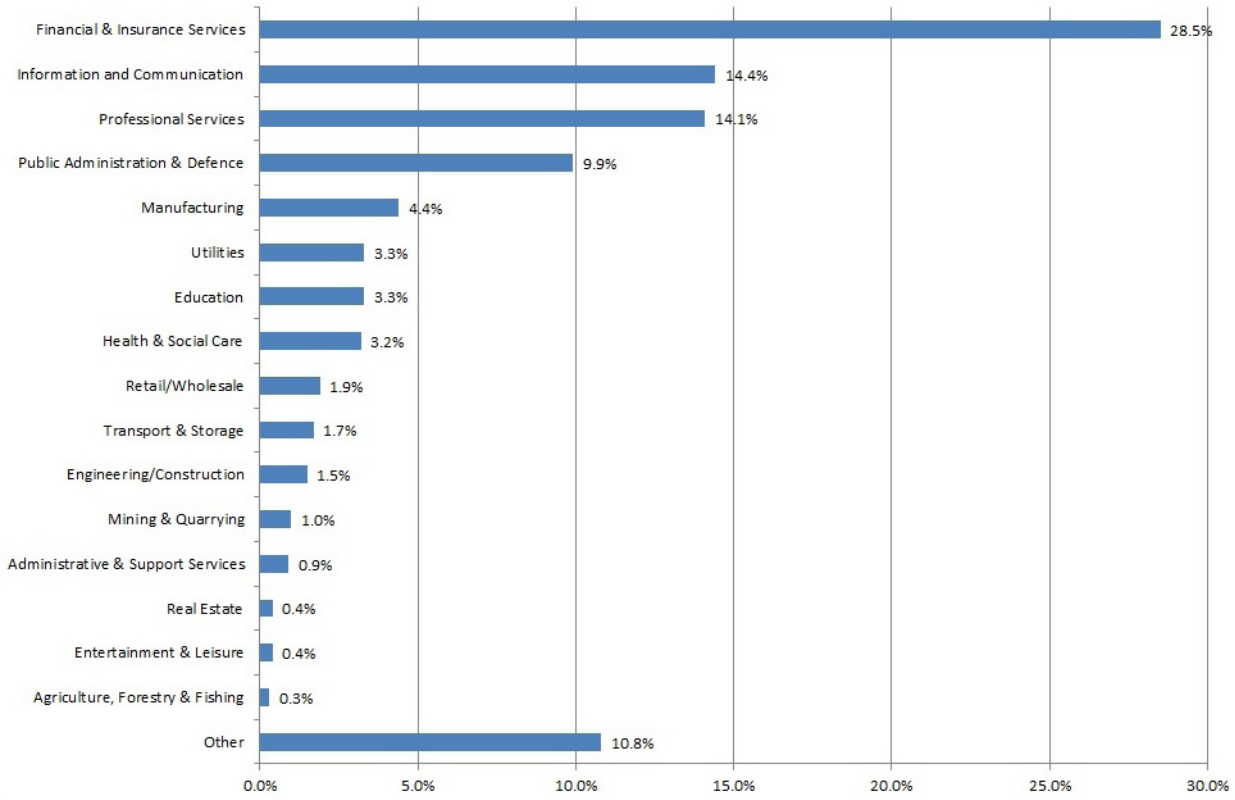

Figure 2.2: Respondent breakdown by primary activity

Figure 2.3 shows the spread of respondents across all sizes of organizations. Those with between 1,001 and 5,000 employees provided the highest percentage of respondents, followed closely by those with under 250 employees.

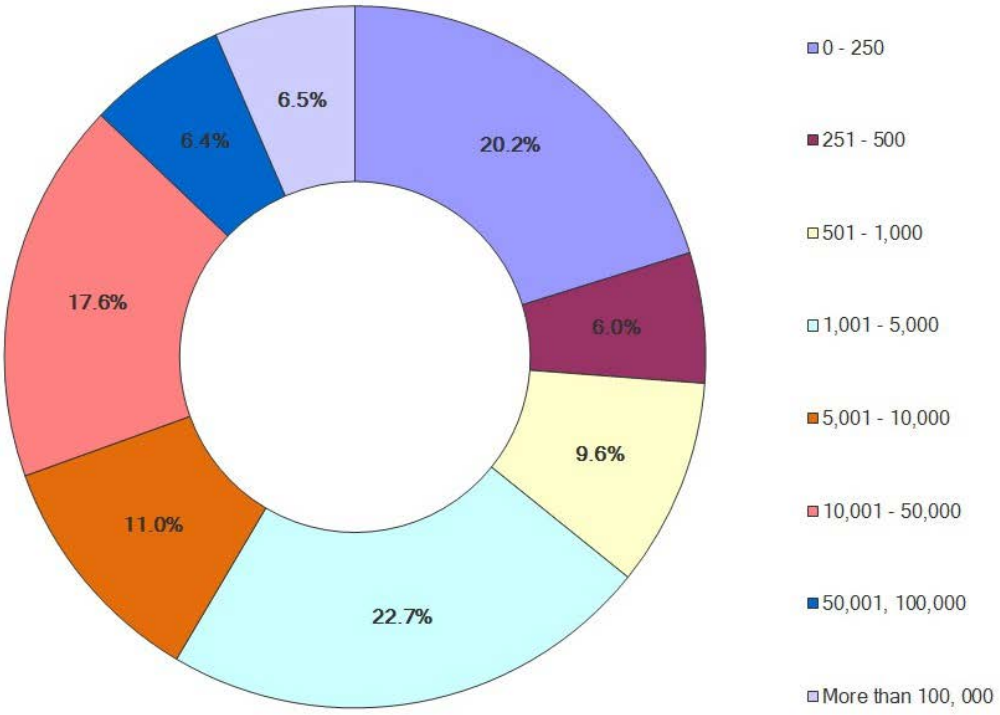

Figure 2.3: Respondent breakdown by organizational size

In addition to the breakdown above, it was noted that about two thirds of respondents (70%) were members of the BCI. This percentage was higher for respondents working in the ***professional services*** (81%) or ***public administration and defence*** (79%) sectors and also for respondents working for organizations with between 5,001 and 10,000 employees (78%) or between 50,001 and 100,000 employees (80%).

3. Top threats in 2014

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

- Unplanned IT and telecom outages
  (77% extremely concerned or concerned)
- Data breach
  (73% extremely concerned or concerned)
- Cyber attack
  (73% extremely concerned or concerned)

It is clear from this that the threat to information systems is considered much more of an issue than the threat to anything else. These three threats are rated significantly higher than the next cluster of threats, which include:

- Adverse weather
  (57% extremely concerned or concerned)
- Interruption to utility supply
  (56% extremely concerned or concerned)
- Security incident
  (53% extremely concerned or concerned)

Case study: interruption to utility supply

Arguably one of the most high profile interruptions to utility supply during 2013 took place at the Superbowl, as early on in the third quarter, the stadium was cast into darkness. This may have been an extremely localized incident but it was one that had the potential to cause major disruption, not just in financial costs, but also in terms of reputation.

The Superbowl is the climax to the NFL season and is watched by over 100 million people in the US, in addition to the viewers in 80 other countries across the world who all screen it live. The power was out for only 22 minutes and the game was delayed for a total of 34 minutes – not long but exceptionally significant.

With an audience of this size, the Superbowl is a big money event with advertisers paying $4million for a 30 second commercial. With no action on the field however, viewers soon start to switch off. If the advertisers felt like they lost out and did not get value for money, they may be reluctant to return next time.

What would the cost be to your organization, direct or indirect, if power went out either for a short period of time or for longer?

Reputation-wise, it was just as costly, not just to the NFL but also to the stadium owners and the city of New Orleans. To suffer such an embarrassing event at such a high profile event, plenty of questions were asked as to how it could happen, especially considering the investment made in order to prepare the stadium for the Superbowl.

If a power failure can occur at one of the most high profile events in the world, at a venue that had undergone significant investment to prevent such an incident, what are the chances of it happening at your organization?

Legally, it could also have been costly. When the lights went out, the Baltimore Ravens were winning comfortably, having built a 28–6 over the San Francisco 49ers. When the game restarted, the 49ers soon cut that lead down to 28-23. In the end the Ravens won 34-31 so it remains a hypothetical point, but given the tension on the touchline and the accusations made after the game, given the ever more litigious world that we live in, it doesn't take much imagination to consider the legal ramifications had the 49ers overturned Baltimore's lead.

If your organization was unable to deliver the service you had been contracted to do, would you open yourselves up to legal action?

The lesson from Superbowl XLVII is that power failures can happen to any organization no matter what investment is put into preventing them. To avoid financial, reputational or perhaps even legal damage, organizations must have processes in place that allow them to respond.

Figure 3.1 provides a breakdown against each of the 29 threats offered in the survey. They are ranked by level of concern, with the number of people stating they were extremely concerned dictating the final position in the table.

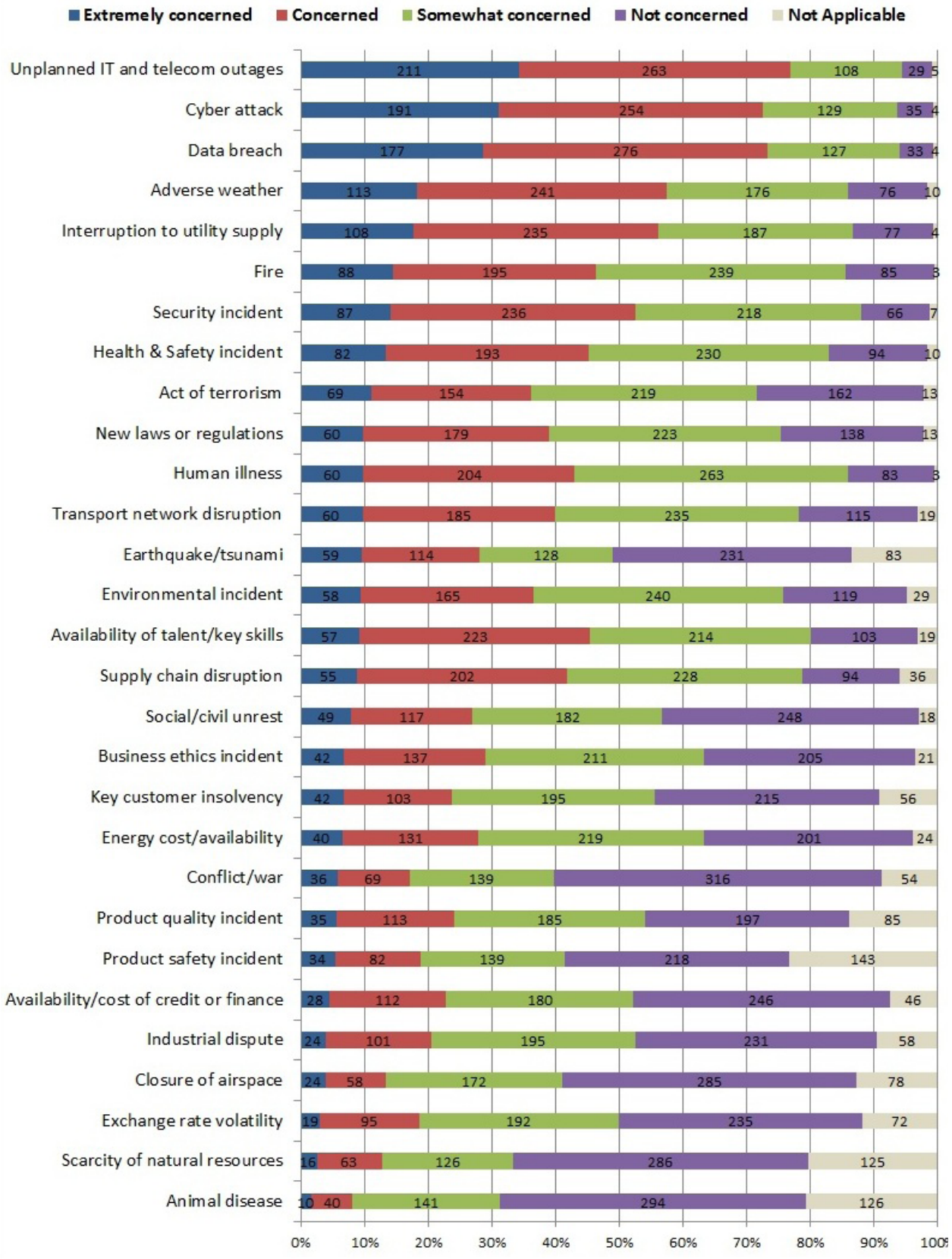

Figure 3.1: Breakdown of threats

Changes from last year's survey

Figure 2.3 reveals that within the top ten, ***cyber attack*** (3->2), ***adverse weather*** (5->4) and ***fire*** (7->6) all moved up a place with ***health and safety incident*** moving up two places (10->8). Going the other way, ***data breach*** (2->3), ***interruption to utility supply*** (4->5) and ***security incident*** (6->7) all moved down a place. ***New laws or regulations*** entered the top ten in tenth place (11->10) while exiting the top ten with the biggest change from the previous year was ***supply chain disruption*** (8->16).

The fall of supply chain disruption as a perceived major threat comes as a surprise given the nature of the potential disruption caused, an area of concern demonstrated in the BCI's Annual Supply Chain Resilience Report. The 2013 Supply Chain Resilience Survey revealed that 75% of respondents experienced at least one supply chain disruption during the previous year with 42% of this disruption originating below the immediate supplier. The cost of this was significant as 15% experienced an annual loss in excess of €1M while 9% experienced a single event that resulted in a loss in excess of €1M.

Outside of the top ten, other incidents gaining prominence include ***transport network disruption*** (15->12), ***environmental incident*** (17->14), ***social unrest*** (20->17) and ***key customer insolvency*** (24->19). Moving the other way, ***product quality incident*** (18->22), ***availability/cost of credit or finance*** (19->24) and ***exchange rate volatility*** (23->27) all became lesser concerns. These latter two are probably as a result of the improving economic outlook.

In addition to the 29 options given, some respondents offered their own ideas as to what the main threats could be in the future.

Crime was frequently mentioned, particularly ***violent crime involving firearms*** or ***kidnapping***. Staying with the crime theme, ***copyright infringement*** was also considered a threat. This is becoming more of an issue in the digital age as it is far easier to pass on information regardless of whether it is copyright protected.

From a financial perspective, ***decreasing budgets*** and therefore a reduction in the ability to combat any threat was considered a threat in itself, as was ***major restructuring within organizations***, presumably as significant change can often lead to uncertainty.

Politically, there were a lot of concerns raised regarding the EU and the increasing level of regulation that it imposes and in the United Kingdom the uncertainty surrounding the outcome of the independence referendum in Scotland.

One respondent highlighted that a train carrying radioactive waste frequently traveled close by their office and this must be considered a threat as any incident could result in large areas being evacuated or cordoned off for long periods of time. This offers an ideal example of why organizations must consider localized threats that are more relevant to them, rather than base their horizon scan on generic threats.

Perception of threats is almost always dependent upon recent history. For example, for the first time in this series of reports, Japan, New Zealand and India all feature heavily due to an increased number of respondents from each of these countries.

Both Japan and New Zealand have suffered as a result of natural disasters in recent years and this was evident in the survey with respondents from both countries rating earthquake/tsunamis higher than any digital threat.

India has undergone turmoil with regard to the terrorist threat so security incident featured highly for them.

Similarly Canada was one of the few countries to include adverse weather as one of its top three threats, perhaps the result of the recent polar vortex affecting North America creating extremely cold temperatures.

Earthquakes and tsunamis: Japan and New Zealand's experiences of threats

In 2011 an earthquake measuring 9.0 on the Richter Scale shook the Pacific coast of Japan, the most powerful earthquake ever to hit the country. A consequence of the earthquake was a tsunami with waves of up to forty metres that struck the north east coast of Honshu.

The immediate aftermath of the disaster was almost 16,000 deaths, nearly quarter of a million buildings severely damaged and over half a million buildings partially damaged. Parts of the region's infrastructure were devastated with many roads and railways damaged and a dam collapsed.

Perhaps the most notable effect of the tsunami was the damage to the Fukushima Daiichi Nuclear Power Plant where at least three nuclear reactors suffered explosions due to a cooling system failure. Large evacuation zones were set up with many residents being displaced.

To place a monetary figure on such damage is no easy task, but the World Bank estimated that the economic cost was US$235 billion.

During the same year, Christchurch in New Zealand also suffered the impact of an earthquake. It was not the most powerful that New Zealand had experienced but the proximity of the epicentre to a major city where buildings had already been weakened as a result of an earthquake the previous year meant the damage was significant.

At the time it was estimated that the cost to the insurers was in the region of NZ$15 billion (US$12.5 billion), although more recent estimates have put the total cost closer to NZ$40 billion (US$33.5 billion).

The security threat: India's perspective on terrorism

In 2008, a series of shooting and bombing attacks in the Indian city of Mumbai lasted for four days and resulted in the deaths of 164 people. Terrorism is not unheard of in India but the scale of this attack was previously unimaginable, so much so that it is now often described as India's 9/11.

The physical damage caused by such events do not take long to recover from but the fear factor that they bring usually lasts for much longer. The reputational damage and the economic damage do take time to recover from.

4. Trend analysis

In addition to better understanding how organizations determine the threats they face, a further component of the Horizon Scan was assessing the extent to which long term analysis was conducted on trends and uncertainties.

Overall, 71% of respondents confirmed that their organization did perform trend analysis while 22% stated their organization did not, as shown in Figure 4.1.

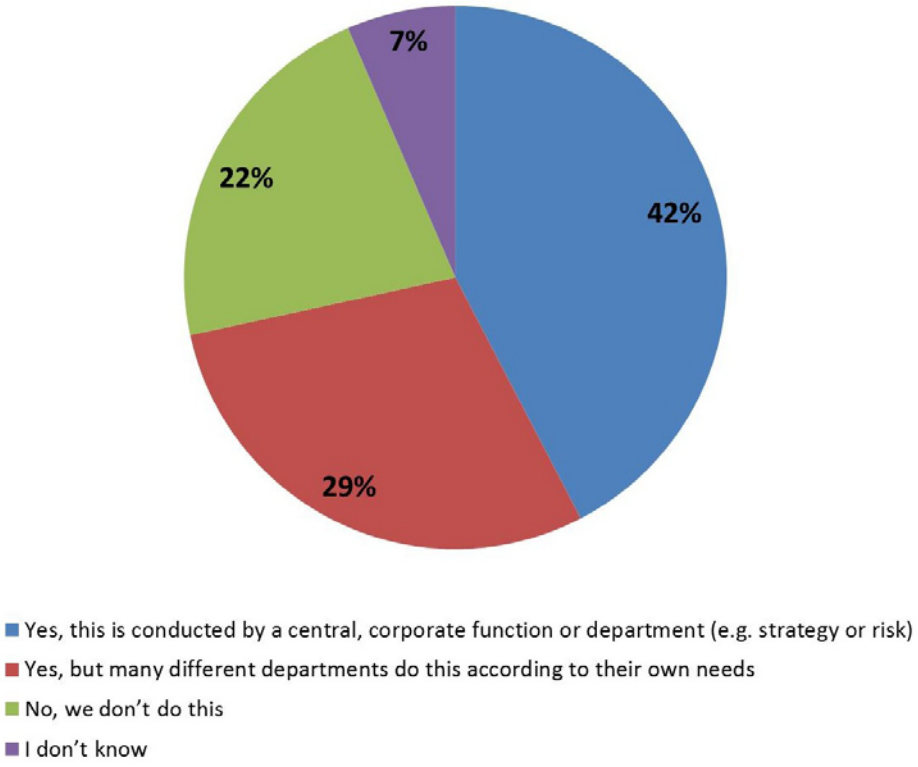

Figure 4.1: Organizations conducting a trend analysis

As a follow up question, the survey asked whether respondents drew upon the outputs of the trend analysis for their business continuity programme; for example as a basis for exercise planning or to consider areas of future capability. Overall 34% of survey respondents did not have access to this information while 4% do not see any value in it.

When you take into account only those who stated their organization did perform a trend analysis, an astonishing 20% still did not have access to this information even though it exists. Figure 4.2 shows that 53% are aware and use the outputs, while 26% are involved in developing the analysis in the first place. Interestingly, only 1% of respondents whose organization did conduct a trend analysis failed to see the value of such information.

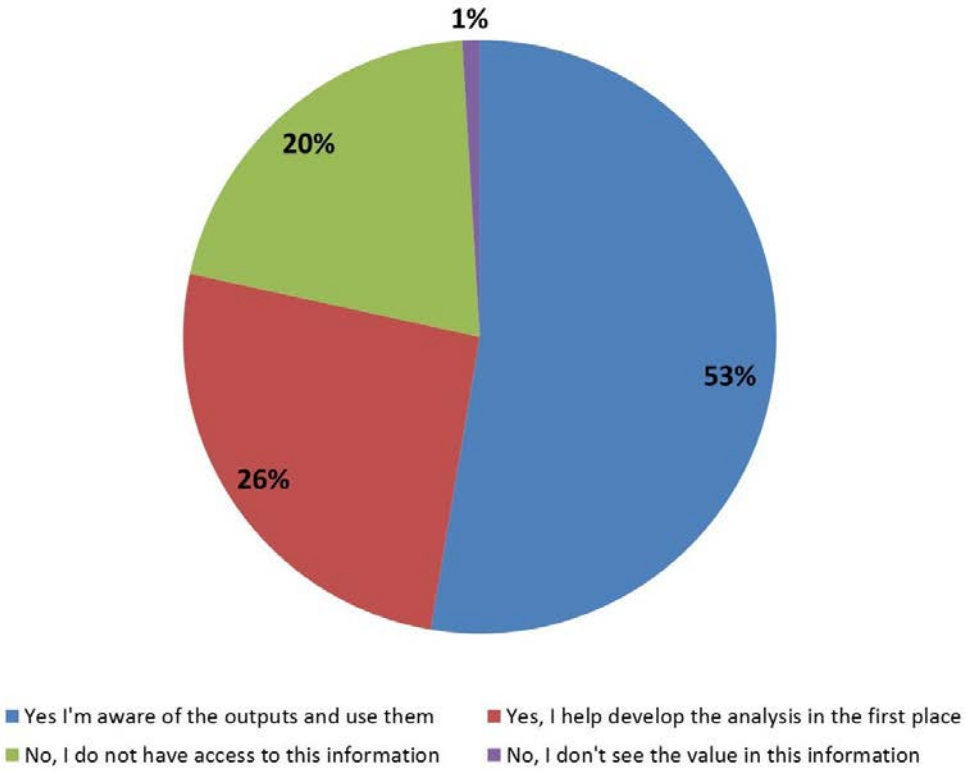

Figure 4.2: Organizations using their trend analysis

Top trends

The survey asked whether any of the 17 identified trends, emerging trends or uncertainties were on the respondent's radar for evaluation in terms of their business continuity implications. The top five were:

1. Use of the internet for malicious attacks (73%)
2. Influence of social media (63%)
3. New regulations and increased regulatory scrutiny (55%)
4. Prevalence and high adoption of internet-dependent services (48%)

=5. Potential emergence of a global pandemic (45%)

=5. Increasing supply chain complexity (45%)

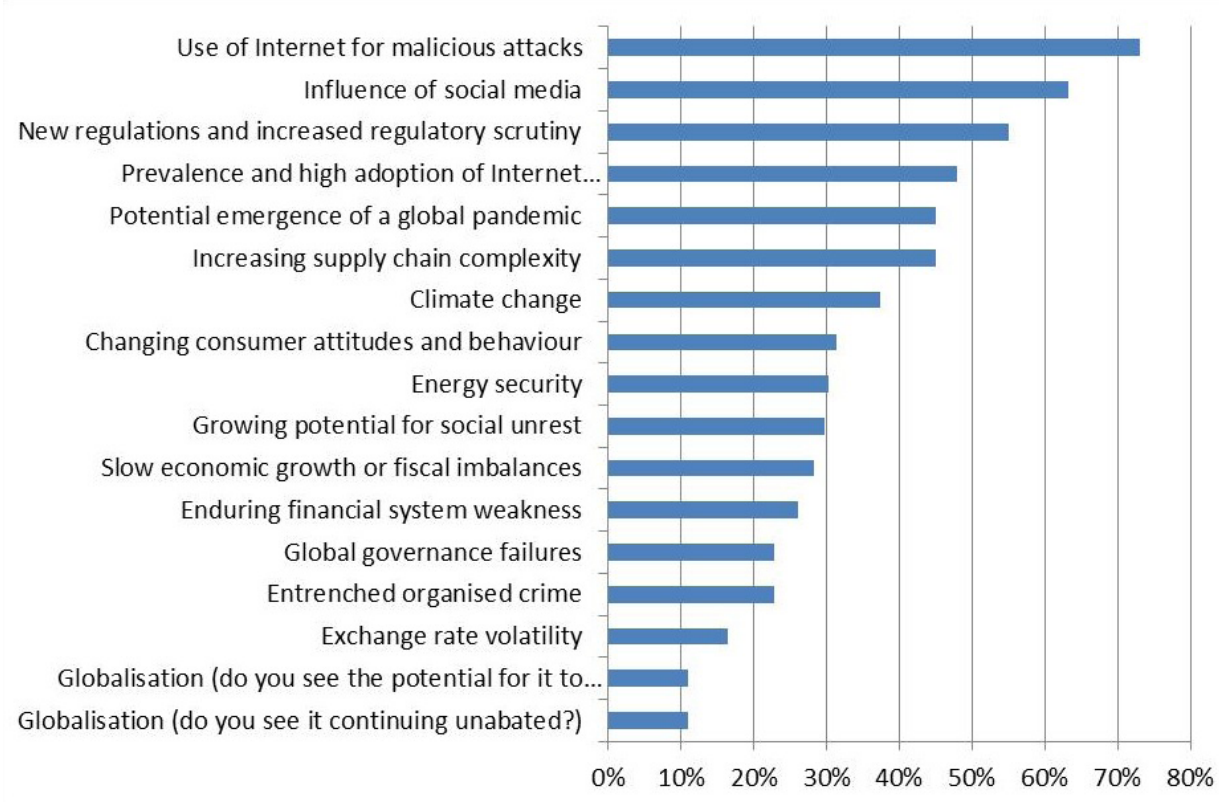

Figure 4.3: Breakdown of trends

The leading trend is the use of the ***internet for malicious attacks*** with 73% of respondents stating that it is on their radar. The strength of sentiment behind this trend is significant. Even when considered on a sector or organizational size basis, its prominence is confirmed. Only those in the health and social care and manufacturing sectors did not rate it highest, although it was still in their top three.

For organizations with between 501 and 1,000 employees, the use for the ***internet for malicious attacks*** was marginally in second place, however for all other sizes of organization it was top.

Geographically there was a bit more variation. Canada, Japan, India, Germany, New Zealand, and the United Arab Emirates were countries who all rated other trends higher along with the regions of Middle East and North Africa and Central and South America. These higher rated trends included ***climate change***, ***new regulations and increased regulatory scrutiny, potential emergence of a global pandemic, influence of social media, supply chain complexity*** and ***energy security***. This perhaps demonstrates that it is location rather than size or primary activity that is important to organizations when determining threats and trends.

The ***influence of social media*** featuring so high for the second year running is no surprise given the impact it can have. Loss of reputation is becoming increasingly important in terms of business continuity planning and social media can have a sizeable influence on reputation, whether it is justified or not. Of course it is not only a negative influence as organizations can use social media to build a positive reputation.

New regulations and increased regulatory scrutiny is high, reflecting that many respondents operate in highly regulated sectors, such as ***financial and insurance services***, where attempting to align the organization an increasing number of regulations can cause severe disruption.

The prevalence of high adoption of ***internet dependent services*** again shows the impact the digital world can have on an organization. As organizations rely more heavily on developing technology, there is always an increased risk of there being more things to go wrong.

Increasing ***supply chain complexity scores*** 45% and this trend is rated significantly higher in specific sectors such as ***manufacturing***. It is perhaps a surprise that supply chain complexity features so highly as a trend while supply chain disruption has reduced significantly as a threat.

Making it into the top five is the ***potential emergence of a global pandemic*** reflecting the higher threat score given to ***human illness***.

5. Investment in business continuity

The survey reveals a greater percentage of respondents expressing concern or extreme concern with the top threats than previous years, so with these threats seemingly on the rise, it might be expected that the investment required to combat them would also increase.

The overall picture however, is that investment is being maintained at current levels for the vast majority of organizations. As Figure 5.1 shows, only 18% of organizations are increasing their budget (compared to 22% in the previous survey) and 11% are actually decreasing their budget (compared to 14% in the previous survey). This suggests that for the majority of organizations, little has changed in the perceived threat levels to justify any change in expenditure.

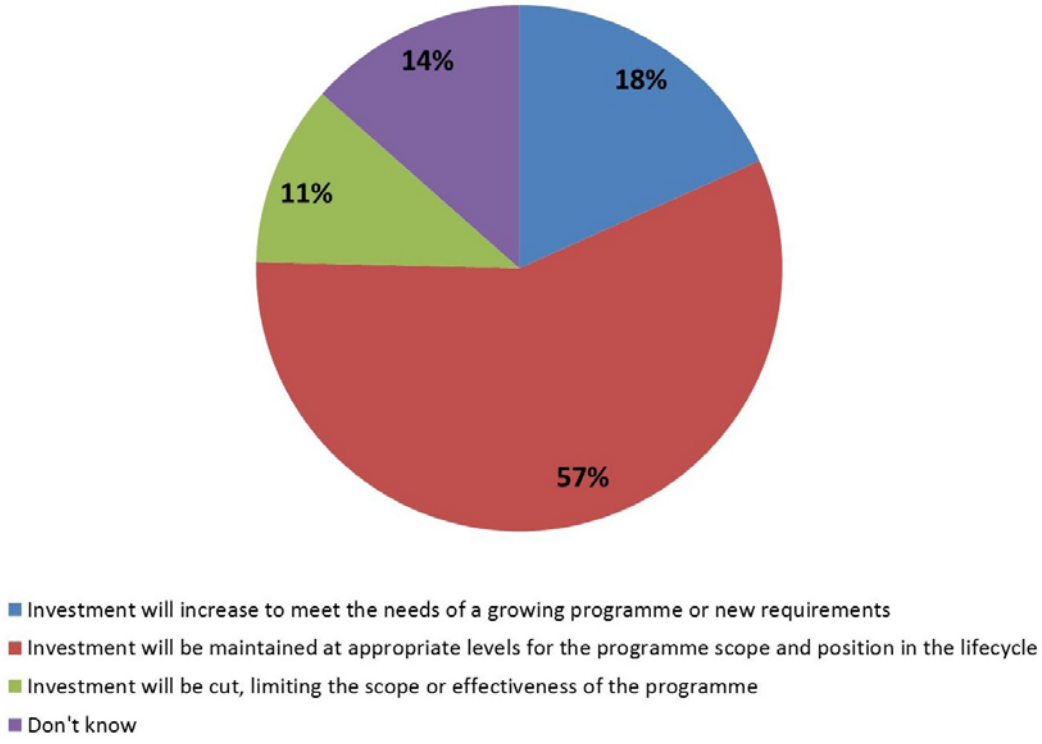

Figure 5.1: Investment in business continuity

There are variations in this pattern depending on the primary activity, geographical location and size of the organization.

As Figure 5.2 shows, organizations working in the ***information and communication*** sector are more likely to increase their budget, while those in the ***public administration and defence sector*** are more likely to cut their budget. This perhaps reflects the greater propensity of public sector organizations to feel the burden of the financial crisis and make cuts.

Those in the ***manufacturing*** industry are less likely to maintain their budget at current levels with a relatively equal split between those planning to increase their budget and those choosing to cut their budget.

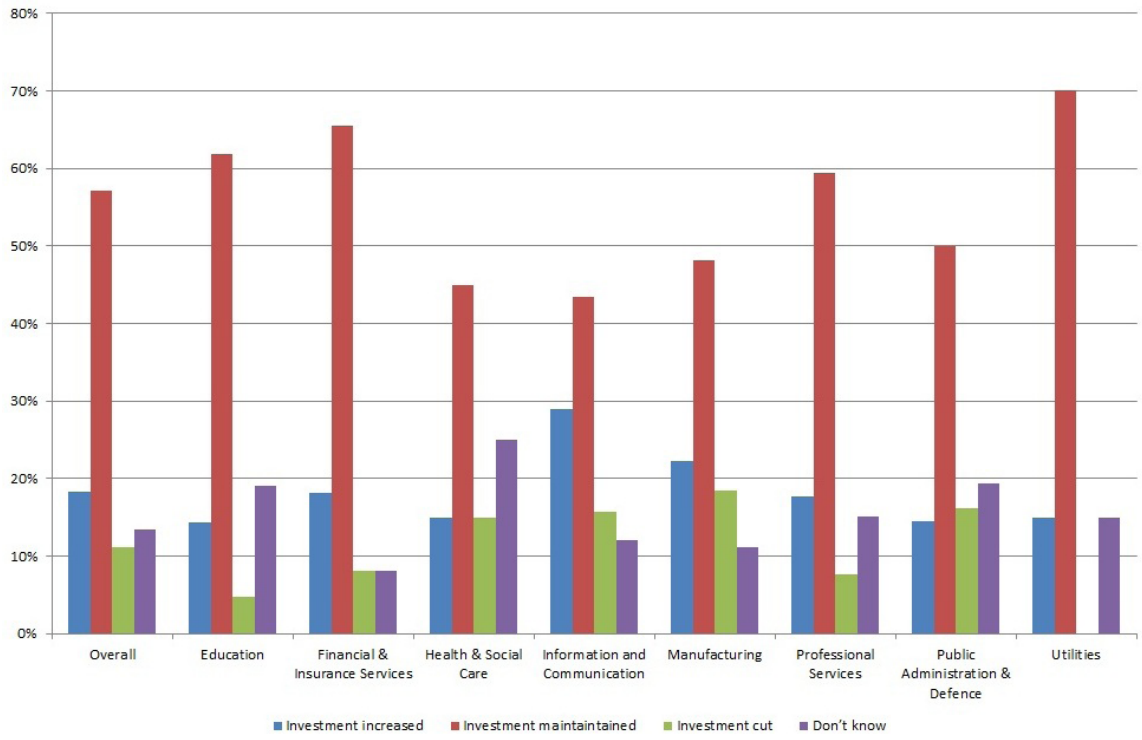

Figure 5.2: Investment in business continuity broken down by primary activity

Figures 5.3 and 5.4 show that there were more variations depending on geographic location. Organizations in the United Kingdom were less likely to increase their budgets, something that goes against the grain for the rest of Europe who are more likely than many areas to increase their budget. Those in Sub Saharan Africa are also more likely to increase their budget. South and Central America along with Canada appear more likely to cut their budgets.

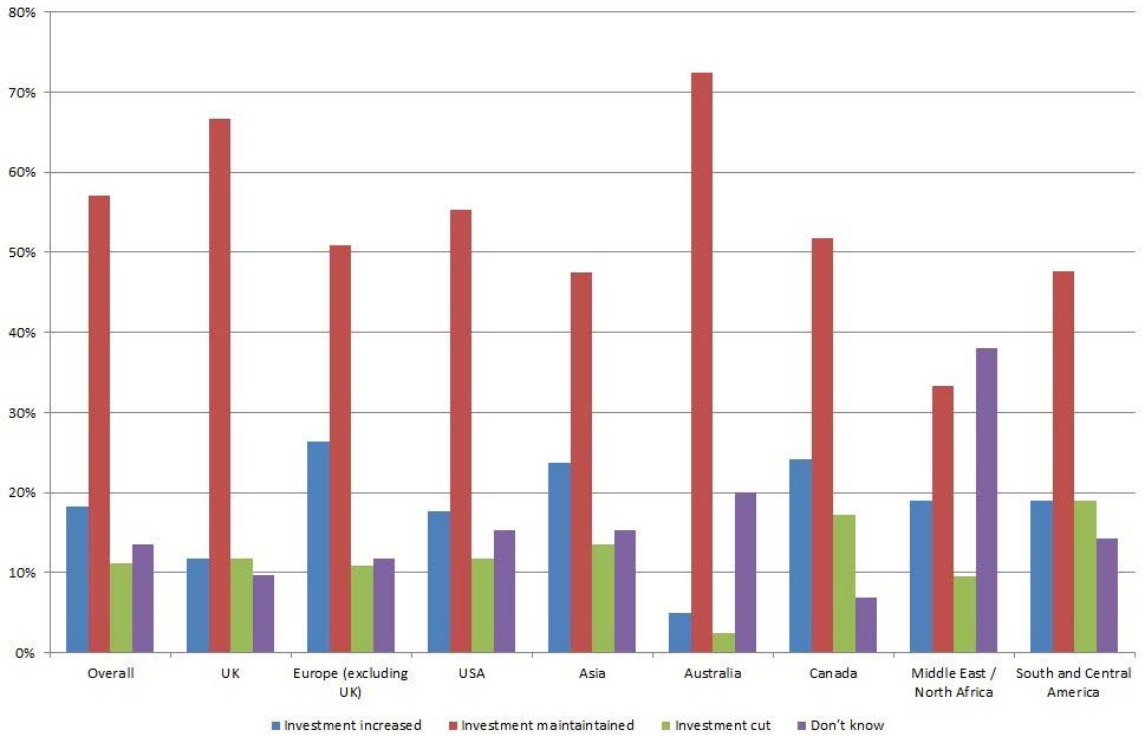

Figure 5.3 Investment in business continuity broken down by geography (1)

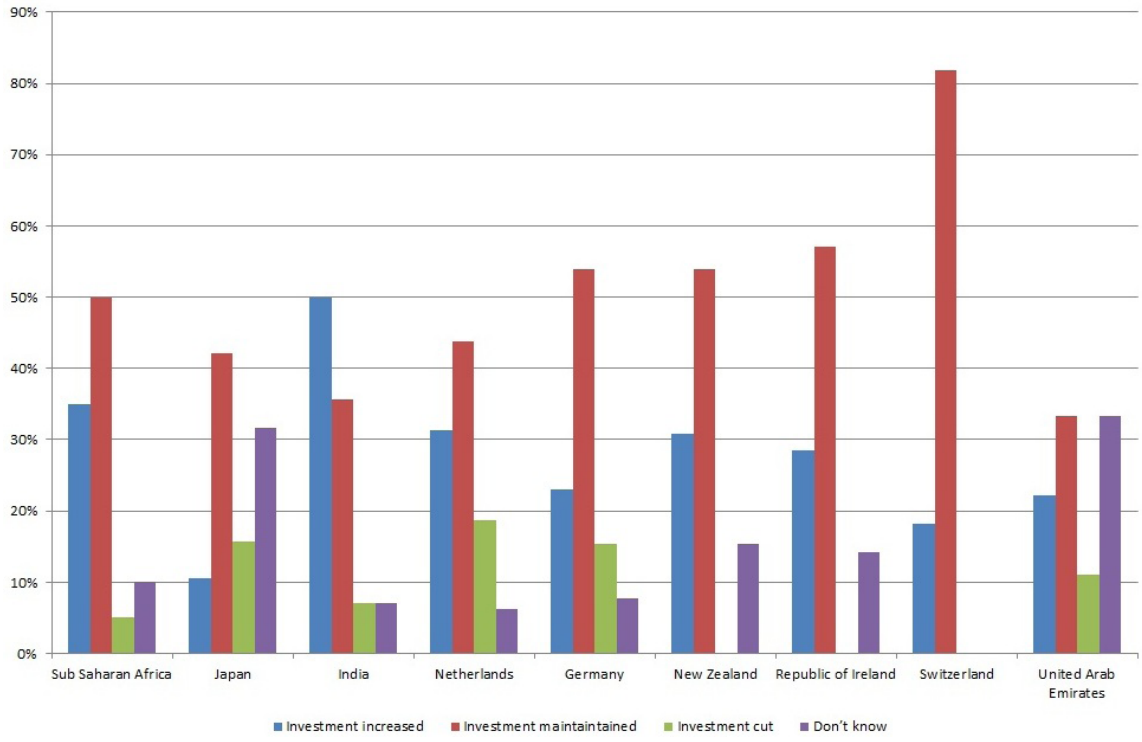

Figure 5.4 Investment in business continuity broken down by geography (2)

Moving on to organizational size, Figure 5.5 doesn't really reveal any surprises. Small organizations are more likely to make cuts as they strive to reduce their overhead. Larger organizations are more likely to increase their budgets as they perhaps have a greater capacity to absorb these costs.

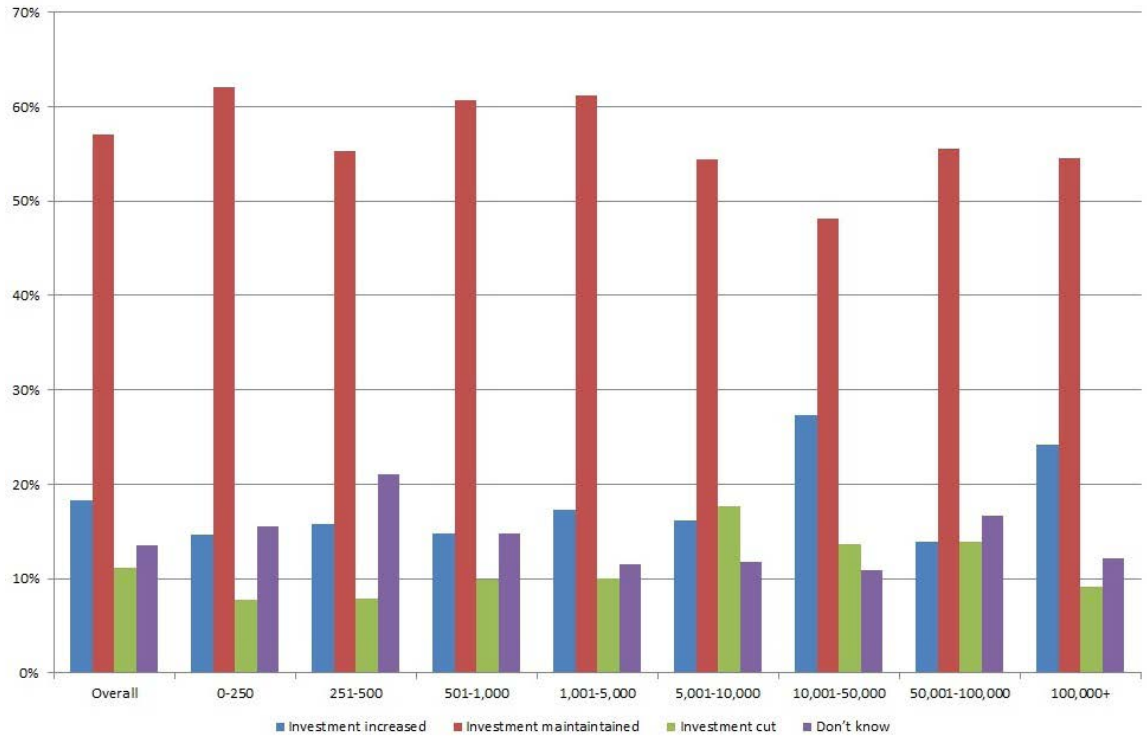

Figure 5.5 Investment in business continuity broken down by organization size

6. ISO 22301 as a framework for BCM programme

It was noted that less than a half of respondents (44%) currently use ISO 22301 as a framework for their business continuity management programme although about a quarter (24%) claimed they were planning to adopt it as a framework during 2014.

As Figure 6.1 shows, there was a significant variation between geographic locations, although it should be noted that the higher the number of respondents any particular region had, the closer they came to the average. Respondents from Canada and Netherlands were far less likely, on average, to use ISO 22301 as a framework although that may change next year for the latter as the figures did show a large percentage of respondents from the Netherlands planning to adopt ISO 22301 during 2014.

Finally the figures show that respondents from Sub Saharan Africa were more likely to use ISO 22301 as a framework.

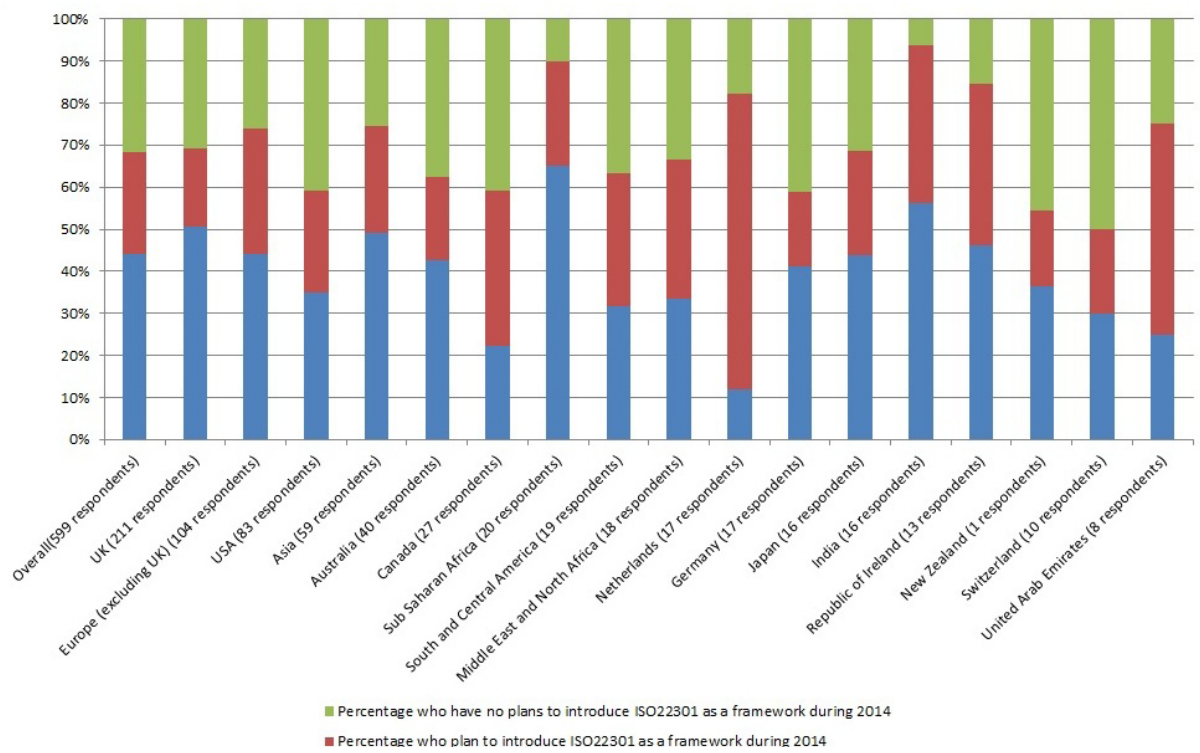

Figure 6.1: Use of ISO 22301 as a BCM framework broken down by geography

Figure 6.2 shows less variation between organizations depending on their primary activity. Those in the *manufacturing* sector were less likely to use ISO 22301 while those within the *information and communications* and *public administration* and *defence* sectors were more likely to use ISO 22301.

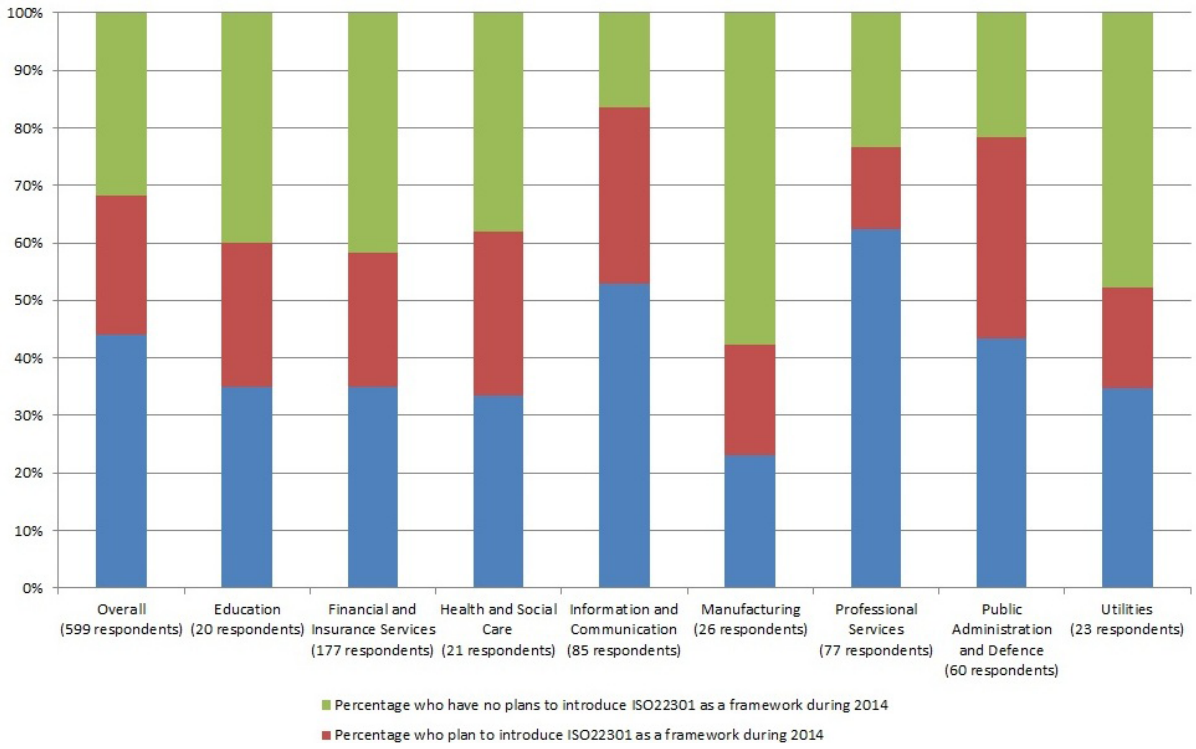

Figure 6.2: Use of ISO 22301 as a BCM framework broken down by primary activity

Similarly to primary activity, Figure 6.3 shows little variation between the size of the organization and its likelihood to adopt ISO 22301.

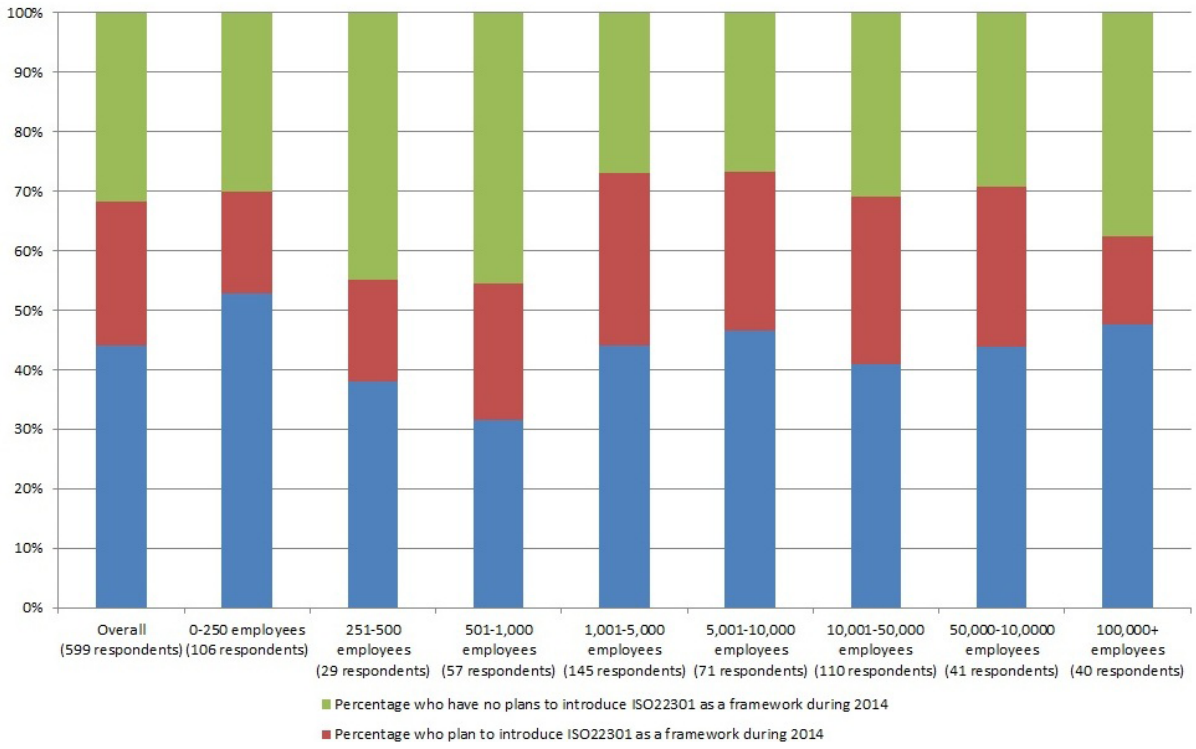

Figure 6.3: Use of ISO 22301 as a BCM framework broken down by organization size

7. Comparison by primary activity of the organization

	Education	Financial and insurance Services	Health and social care	Information and communication	Manufacturing	Public administration & defence	Professional services	Utilities
Number of respondents	23	196	22	99	30	97	68	23
Percentage of respondents from UK, USA, Canada or Australia	74%	53%	73%	50%	43%	52%	76%	74%
Percentage of respondents who conduct a trend analysis	52%	65%	59%	64%	63%	54%	63%	65%
Percentage of those above who have no access to final output	33%	23%	15%	35%	21%	12%	28%	27%
Top three Threats	1 Unplanned IT or telecoms outages 2 Cyber attack 3 Security incident	1 Unplanned IT or telecoms outages 2 Data breach 3 Cyber attack	1 Unplanned IT or telecoms outages 2 Human illness 3 Health and safety incident	1 Cyber attack 2 Unplanned IT or telecoms outages 3 Data breach	1 Supply chain disruption 2 Product quality incident =3 Unplanned IT or telecoms outages =3 Cyber attack =3 Data breach	1 Data breach 2 Cyber attack 3 Unplanned IT or telecoms outages	1 Unplanned IT or telecoms outages 2 Cyber attack =3 Adverse weather =3 Data breach	1 Unplanned IT or telecoms outages 2 Cyber attack 3 Data breach
Top three trends	1 Use of the internet for malicious attacks 2 New regulations and increased regulatory scrutiny 3 Influence of social media	1 Use of the internet for malicious attacks 2 New regulations and increased regulatory scrutiny 3 Influence of social media	1 Potential emergence of a global pandemic 2 Influence of social media 3 Use of the internet for malicious attacks	1 Use of the internet for malicious attacks 2 Influence of social media 3 High adoption of internet dependent services	1 Increasing supply chain complexity 2 Influence of social media 3 Use of the internet for malicious attacks	1 Use of the internet for malicious attacks 2 Influence of social media 3 High adoption of internet dependent services	1 Use of the internet for malicious attacks 2 Influence of social media 3 Potential emergence of a global pandemic	1 Use of the internet for malicious attacks 2 Energy security =3 New regulations and increased regulatory scrutiny =3 Influence of social media

Table 1: Results broken down by primary activity

Table 1 shows the breakdown of the results depending on the primary activity of the organization. Eight primary activities were featured as those that had a sufficient number of respondents to justify segmenting them. The table shows that there are a few variations between the threats and trends depending on the primary activities.

Security incident just makes it in to the top three for ***education***, the only one of the eight featured activities where it appears. It would be logical to suggest that this is due to the number of high profile incidents that have occurred in the US and the fact that schools are often considered an 'easy target'.

Health and safety incident and ***human illness*** both appear only once and this is within the ***health and social care*** sector. This is presumably because this sector contains (not employs) a large number of vulnerable people who would be more susceptible to the effects of an incident of this type.

Supply chain disruption and ***product quality incident*** both appear as a major threat for the ***manufacturing*** industry and this can be expected. This type of industry tends to have longer more complex supply chains and recent examples of product quality incidents have shown to be both expensive in terms of cost and reputation. There are several car manufacturers who have had to undergo embarrassing product recalls and airlines that have grounded flights because equipment is deemed unsafe. Perhaps it is safe but the potential for reputational damage is too great to take the chance.

Adverse weather appears as a threat fo***r public administration and defence*** and it could be assumed that this is because this sector would largely be responsible for any clear up operation required as a result of this threat materializing. This is also the case the ***potential emergence of a global pandemic*** where the ***health and social care*** and ***public administration and defence*** sectors both feature these as a trend.

8. Comparison by geographic location of the organization

	UK	Europe (excluding UK) [1]	USA	Asia [2]	Australia	Canada	Middle East/ North Africa [3]	South and Central America [4]
Number of respondents	227	122	93	74	47	31	25	24
Top three Threats	1 Unplanned IT or telecoms outages 2 Cyber attack 3 Data breach	1 Unplanned IT or telecoms outages 2 Cyber attack 3 Data breach	1 Cyber attack 2 Unplanned IT or telecoms outages 3 Data breach	1 Data breach 2 Unplanned IT or telecoms outages =2 Human illness	1 Data breach 2 Cyber attack 3 Unplanned IT or telecoms outages	1 Unplanned IT or telecoms outages 2 Adverse weather 3 Data breach	1 Data breach =2 Availability of talent/key skills =2 Fire =2 Cyber attack =2 Health and safety incident	=1 Unplanned IT or telecoms outages =1 Availability of talent/key skills =1 New laws or regulations
Top three trends	1 Use of the internet for malicious attacks 2 Influence of social media 3 Supply chain complexity	1 Use of the internet for malicious attacks 2 Influence of social media 3 New regulations and increased regulatory scrutiny	1 Use of the internet for malicious attacks 2 New regulations and increased regulatory scrutiny 3 Influence of social media	1 Use of the internet for malicious attacks 2 Influence of social media 3 Potential emergence of a global pandemic	1 Use of the internet for malicious attacks 2 Influence of social media 3 High adoption of internet dependent services	=1 Climate change =1 Influence of social media 3 High adoption of internet dependent services	1 New regulations and increased regulatory scrutiny 2 Use of the internet for malicious attacks 3 Influence of social media	=1 Increasing supply chain complexity =1 Influence of social media =1 New regulations and increased regulatory scrutiny

1 Europe (excluding UK) consists of 28 countries including: Albania, Andorra, Austria, Belgium, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Ireland, Isle of Man, Italy, Jersey, Malta, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, Slovenia, Spain, Sweden, Switzerland and Turkey.

[2] Asia consists of 13 countries including: China, Indonesia, India, Japan, Korea, Kazakhstan, Macao, Malaysia, Philippines, Pakistan, Singapore, Thailand and Vietnam.

[3] Middle East / North Africa consists of eight countries including: Egypt, Iran, Iraq, Kuwait, Qatar, Saudi Arabia, Tunisia and United Arab Emirates.

[4] South and Central America consists of nine countries including: Argentina, Brazil, Chile, Colombia, Ecuador, Guatemala, Mexico, Peru and Venezuela.

Table 2: Results broken down by country/region (1)

Table 3: Results broken down by country/region

	Sub Saharan Africa [1]	Japan	India	Netherlands	Germany	New Zealand	Republic of Ireland	Switzerland	United Arab Emirates
Number of respondents	23	23	19	19	19	14	14	12	10
Top three Threats	=1 Interruption to utility supply =1 Fire =1 Cyber attack	1 Earthquake/ tsunami 2 Data breach 3 Human illness	1 Interruption to utility supply =2 Data breach =2 Security incident	1 Cyber attack 2 Unplanned IT or telecoms outages =2 Data breach	1 Unplanned IT or telecoms outages 2 Data breach 3 Cyber attack	=1 Earthquake/ tsunami =1 Cyber attack =3 Adverse weather =3 Interruption to utility supply	=1 Unplanned IT or telecoms outages =1 Cyber attack 3 Interruption to utility supply	1 Cyber attack =2 Health and safety incident =2 Data breach	=1 Availability of talent / key skills =1 Cyber attack =1 Data breach
Top three trends	1 Use of the internet for malicious attacks 2 Influence of social media =3 Slow economic growth or fiscal imbalances =3 High adoption of internet dependent =3 Growing potential for social unrest	1 Potential emergence of a global pandemic =2 Climate change =2 Increasing supply chain complexity =2 Use of the internet for malicious attacks	=1 Climate change =1 New regulations or increased regulatory =1 Potential emergence of a global pandemic =1 Growing potential for social unrest =1 Use of the internet for malicious attacks	1 Use of the internet for malicious attacks 2 Influence of social media 3 New regulations or increased regulatory scrutiny	1 Energy security 2 New regulations or increased regulatory scrutiny =3 Increasing supply chain complexity =3 Influence of social media	1 Influence of social media 2 Use of the internet for malicious attacks 3 High adoption of internet dependent services	1 Use of the internet for malicious attacks =2 Increasing supply chain complexity =2 New regulations or increased regulatory scrutiny =2 High adoption of internet dependent services =2 Influence of social media	1 Use of the internet for malicious attacks =2 High adoption of internet dependent services =2 Influence of social media	1 New regulations and increased regulatory scrutiny 2 Use of the internet for malicious attacks =3 Increasing supply chain complexity =3 Global governance failures

[1] Sub Saharan Africa consists of 11 countries including: Botswana, Ghana, Kenya, Malawi, Maldives, Mauritius, Nigeria, South Africa, Sudan, Uganda and Zimbabwe.

Tables 2 and 3 show the breakdown of the results by region, showing the top three threats and trends for all countries and selected regions with at least ten respondents.

As expected the IT related threats featured heavily (***unplanned IT or telecoms outage, cyber attacks and data breaches***) but there was the occasional variation that stood out. ***Earthquake/tsunami*** is one of those as it was considered a threat by respondents from both Japan and New Zealand for reasons discussed earlier in this report. Respondents from Japan also considered ***human illness*** as a threat and this can again be attributed to the sheer scale of the natural disaster the country suffered from in 2011 its aftermath.

Although it did feature highly in many countries such as the United States and those in South and Central America, it was only respondents from India who included ***security incident*** in their top three threats. Again this is perhaps for reasons that were discussed earlier in this report.

Adverse weather is considered a threat by respondents from Canada. This can be linked to the severe weather that the country has suffered from in recent months, particularly the polar vortex that has affected North America and resulted in extremely low temperatures. ***Adverse weather*** is also thought of as a threat by respondents from New Zealand.

Interruption to utility supplies is a considered a threat by respondents from Sub Saharan Africa where utilities can often be temperamental with electricity for example not always being guaranteed. New Zealand joins Sub Saharan Africa in deeming this a threat and this is perhaps due to the increased likelihood of natural disasters such as earthquakes causing such interruptions.

Fire is considered a threat by respondents from Sub Saharan Africa and in the Middle East and North Africa. This can be attributed to the drier environment and the limited access to water supplies in order to extinguish fires.

Availability of talent/key skills is considered a threat by respondents from South and Central America. This is arguably because many of the skilled workers from this region emigrate to North America or Europe in order to attempt to make a better life for themselves.

For trends, again it is the same ones, those that are largely IT related, that feature so prominently (***use of the internet for malicious attacks, influence of social media and high adoption of internet dependent services***), however there are a few variations.

Asia, and India in particular, see the ***potential emergence of a global pandemic*** as something to watch out for in the future. The continent has had pandemic threats materialize in the past and this is partly aided by the large population, meaning that any disease can spread more readily.

Sub Saharan Africa and India both look at the ***growing potential for social unrest*** as a trend and this is because both regions have gone through political turmoil in recent years with cultural sensitivities often leading to tension.

Supply chain complexity also appears as a trend, especially in the two industrial nations of Germany and Japan, but also in the United Kingdom and South and Central America. As the world becomes increasingly globalized and markets become much larger, this adds even greater stresses to the complexity of the supply chain.

9. Comparison by size of the organization

	1-250 employees	251-500 employees	501-1,000 employees	1,001-5,000 employees	5,001-10,000 employees	10,001-50,000 employees	50,001-100,000 employees	100,001+ employees
Number of respondents	139	41	66	156	76	121	44	45
Percentage of respondents from UK, USA, Canada or Australia	54%	34%	47%	53%	66%	69%	73%	73%
Percentage of respondents who conduct a trend analysis	48%	61%	59%	68%	62%	71%	68%	69%
Percentage of those above who have no access to final output	16%	24%	38%	25%	28%	27%	33%	32%
Top three Threats	1 Data breach 2 Unplanned IT or telecoms outages 3 Cyber attack	1 Data breach =2 Interruption to utility supply =2 Unplanned IT or telecoms outages =2 Cyber attack	1 Unplanned IT or telecoms outages 2 Data breach 3 Cyber attack	1 Unplanned IT or telecoms outages 2 Data breach 3 Cyber attack	1 Unplanned IT or telecoms outages 2 Cyber attack 3 Data breach	1 Unplanned IT or telecoms outages 2 Cyber attack 3 Data breach	=1 Unplanned IT or telecoms outages =1 Cyber attack =1 Data breach	1 Cyber attack 2 Unplanned IT or telecoms outages 3 Data breach
Top three trends	1 Use of the internet for malicious attacks 2 Influence of social media 3 High adoption of internet dependent services	1 Use of the internet for malicious attacks 2 New regulations and increased regulatory scrutiny 3 Influence of social media	1 Influence of social media =2 New regulations and increased regulatory scrutiny =2 Use of the internet for malicious attacks	1 Use of the internet for malicious attacks 2 Influence of social media 3 New regulations and increased regulatory scrutiny	1 Use of the internet for malicious attacks 2 Influence of social media 3 New regulations and increased regulatory scrutiny	1 Use of the internet for malicious attacks 2 Influence of social media 3 New regulations and increased regulatory scrutiny	1 Use of the internet for malicious attacks 2 Influence of social media 3 New regulations and increased regulatory scrutiny	1 Use of the internet for malicious attacks 2 Influence of social media 3 New regulations and increased regulatory scrutiny

Table 4: Results broken down by size of organization

Table 4 show the breakdown of the results by the size of the organization, showing the top three threats and trends for all the different sizes of organization.

This table however, shows little variation with all sizes of organizations having ***unplanned IT and telecoms***, ***cyber attack*** and ***data breach*** within their top three. The only other threat to appear is ***interruption to utility supply*** which appeared in equal second place on the list for organizations with between 251 and 500 employees.

For all but one of the size categories the top three for trends was made up of ***use of the internet for malicious attacks***, ***influence of social media*** and ***new regulations and increased regulatory scrutiny***. The variation was for organizations with fewer than 250 employees who had ***high adoption of internet dependent services*** in their top three rather than new regulations. This is presumably because the smaller an organization is, the harder and more expensive it becomes to keep up with technology.

Tables and figures

This report provides a comprehensive view of the top threats faced by nearly 700 business continuity managers from 82 countries in 2014, along with an analysis of the underlying trends and uncertainties of concern that may cause future disruption.

© 2014 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:** bci@thebci.org

www.thebci.org

mynewsdesk™