Horizon Scan 2015

SURVEY REPORT

Business Continuity Institute

bsi.

BCI Foreword

Lyndon Bird FBCI
Technical Director

I'm delighted that once again the Business Continuity Institute in conjunction with the British Standards Institution is able to publish the results of the annual Horizon Scan survey.

This comprehensive analysis has fast gained a reputation as an essential tool for the business continuity professional. In fact it has become, in my opinion, the definitive report in this field globally. As Technical Director I am proud to be associated with the work that the BCI research team have undertaken.

The diverse problems that the world currently faces range from cybercrime and political unrest to supply chain vulnerabilities and health hazards. This survey shows the vital importance of business continuity professionals understanding such trends and relating them to problems they will inevitably experience in their own organisations. The cyber-attack on Sony pictures just before Christmas 2014 and that on the US Security Services shortly afterwards rapidly acquired the status of a national emergency in the United States with presidential involvement.

It is not surprising therefore that for the first time cyber issues top the list of current threats. In fact the top three are all technology related. However other problems such as the aftermath of the Ebola crisis and terrorist attacks in Paris and Pakistan also are increasingly concerning. The emergence of new terrorist techniques with the self-proclaimed 'Islamic State' in the Middle East and Boko Haram in Africa are creating an increasingly turbulent world where physical and virtual attacks can be combined to devastating effect. No longer can we as business continuity practitioners believe we can resolve all our problems ourselves, we need to work together with our fellow professionals to deal with the complexity of the threats. I think that this annual survey is one of the BCI's most important publications and I hope you share my opinion of its value.

Business Continuity Institute

BSI Foreword

The past year has shone a spotlight on the impact cyber attacks can have upon our society, casting a shadow over the apparent preparedness of the banks and organisations upon which we rely. This is our fourth report with the BCI and it appears the failures of a few are beginning to encourage the majority to pay closer attention to business continuity. However, while awareness is rising, action is still limited.

Cyber risk is now considered to be the top concern for businesses, up from second place in 2014 and third place in 2013. The fastest rising concern however is supply chain disruption, which has increased dramatically since last year, moving up 11 places, with a number of high profile instances forcing businesses to consider their own supply chains and the potential points of weakness. Globalization has brought the world's conflicts, natural disasters and crime much closer to home. It is crucial these risks are recognized and effectively mitigated.

Howard Kerr
Chief Executive

Although it is clear that a growing number of organisations are aware of the potential threats, it is a real concern to me that so many organisations still display resistance in adopting business continuity best practice, particularly when there is an obligation to stakeholders to ensure safeguards are in place. Many businesses are still not analysing the threats to their business continuity, and too many of those that do, are not making proper use of the information once they have it. Tracking near and long-term threats provides organisations of all sizes with an objective assessment of their risks and a way to mitigate and manage them. Importantly, applying this protective discipline across your organisation and then testing your plans, provides business leaders with the tools to not just survive, but thrive in this new world of risk.

bsi.

CONTENTS

Chapter 1

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

The Horizon Scan Survey seeks to consolidate the assessment of near-term business threats and uncertainties based on in-house analysis of business continuity (BC) practitioners worldwide. As a sought-after industry resource, this annual report is used to inform planning assumptions for the year ahead. This report is also a useful tool that feeds into efforts to build organisational resilience through an increased awareness of threats in the near-term.

The data from this report comes from 760 organisations based in 72 countries worldwide. The online survey was open for 8 weeks from November to December 2014. The Annex of this report contains segmentation of the data by industry sector and geographical location. A comparison between small and medium sized enterprises (SMEs)[1] and large business is made for the first time in recognition of the different challenges facing each sector.

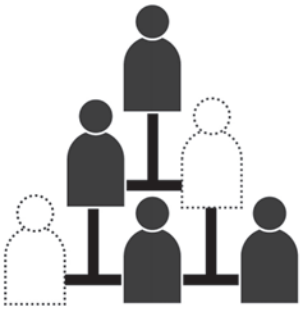
Key Findings

Cyber attacks (82%), unplanned IT and telecommunications outages (81%) and data breach (74%) remain the top threats facing businesses. However, cyber attacks have climbed from third (2013) to second (2014) and now first (2015), reflecting increased concern among BC professionals. Rounding out the top 10 threats are interruption to utility supply, supply chain disruption, security incidents, adverse weather, human illness, fire and acts of terrorism.

Supply chain disruption has risen by 11 places from 16th last year. Security incidents move from seventh to sixth in 2015 whilst acts of terrorism figure in the top 10 for the fourth year running. Human illness figures in the top 10 for the first time since the survey began. Adverse weather has fallen by three places from fourth to seventh in 2015.

Results suggest that the top two trends, the use of the Internet for malicious attacks (81%) and the growing influence of social media (63%), remain unchanged for the third consecutive year. Nonetheless, the growing concern of illnesses such as Ebola have pushed the trend of the emergence of global pandemic from fifth (45% in 2014) to third (59% in 2015).

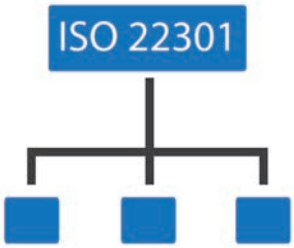
1. SMEs are defined according to EU law as organisations having ≤250 employees and an annual turnover of ≤€50M.



Rounding out the top 10 trends or uncertainties to watch out for are the loss of key employees (59%), new regulations and increased regulatory scrutiny (53%), prevalence and high adoption of Internet-dependent services (49%), increasing supply chain complexity (44%), political change (41%), changing consumer attitudes and behaviour (33%) and growing potential for social unrest (29%).

Slightly more BC professionals report performing trend analysis from 71% to 73%. Nonetheless, the percentage of organisations using the results of trend analysis to inform BCM implementation have fallen from 53% to 43%. Moreover, 22% report not utilising trend analysis at all in their horizon scanning, making it a blind spot for many organisations.

Investment levels for BC are up for more organisations this year at 23% compared to 2014 (18%). Nonetheless, organisations in the health and social care, public, and education sectors are more likely to experience cuts in BC investment. Companies based in Oceania and Central/Latin America are also more likely to cut BC budgets.



More businesses (52% from last year's 44%) use ISO 22301 as a framework for ISO 22301 implementation, with an additional 17% reporting a shift to ISO 22301 this year. This data suggests the growing maturity of the standard.

Further analysis of the data reveals that SMEs are less likely to perform trend analysis compared to large businesses (59% compared to 77%). Only half of SMEs are likely to use ISO 22301 as a framework for BCM implementation. These are significant gaps that may be addressed by measures which facilitate BC planning and standards alignment.

Chapter 2
MAIN REPORT

INTRODUCTION

As a key 'protective discipline', business continuity (BC) ensures organisational resilience by building an effective response to disruptive events. Horizon scanning is a useful BC tool that can provide an objective perspective on threats and uncertainties that may lead to business disruption. This informs – or even confirms – strategy undertaken by businesses to prepare for disruption. The relationship between BC and horizon scanning is shown below (Figure 1).

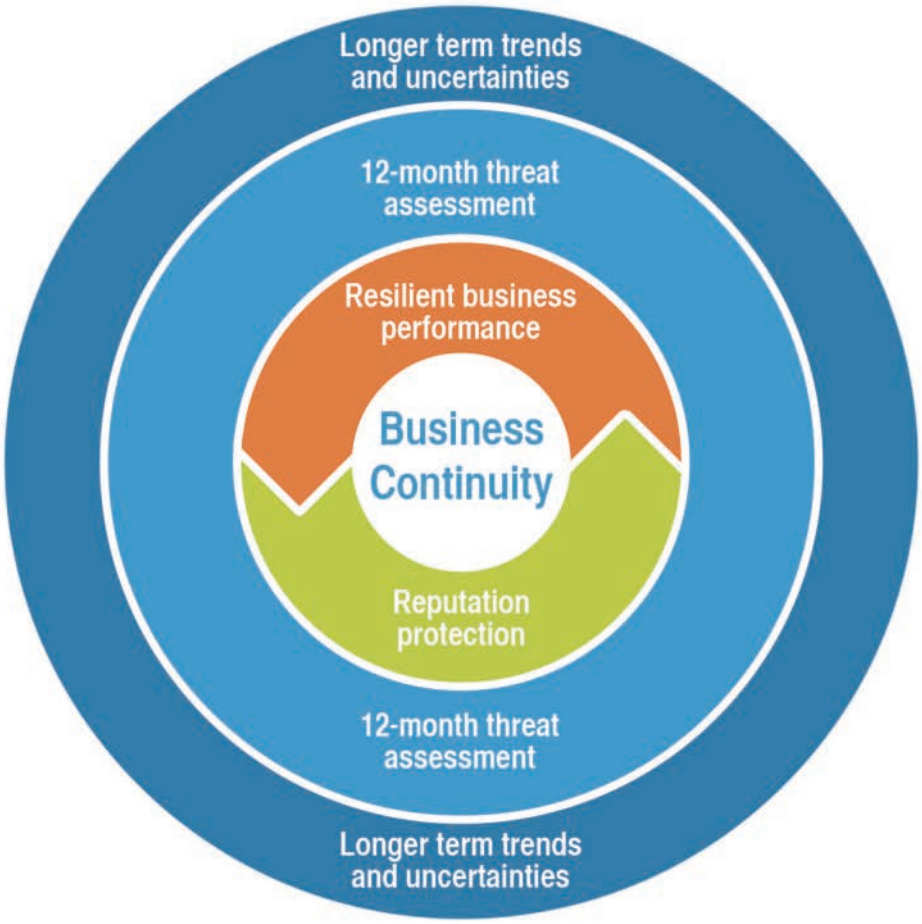


Figure 1. Relationship between BC and horizon scanning

About the Survey

The BCI Horizon Scan Survey, produced in association with BSI, seeks to identify near-term threats on the radar of BC practitioners, benchmark horizon scanning activity and look out for trends that may influence business in the medium- and long-term. For four years, this has been a useful resource for organisations worldwide in planning their BC strategy for the year ahead. The survey commenced on November 2014 and was open for eight weeks. 760 responses from 72 countries have been obtained in this year's survey, an increase of almost 10% from last year.

ANALYSIS

CASE STUDY

Cyber Attacks

On 22nd November 2014, Sony's computer systems were compromised with the release of confidential data including emails from top executives, scripts from upcoming movie projects and films which were then downloaded illegally from the Internet. For a time, employees were forced to work on pen and paper as a result of the incident. Experts acknowledge that the hack was perpetrated by an 'organised group' and estimate the cost at around US$100 million.

References

BBC, 2014. The Interview: A guide to the cyber attack on Hollywood. BBC (online)

Available from: http://www.bbc.co.uk/news/entertainment-arts-30512032

Finkle, J. and Richwine, L., 2014. Sony investigator says cyber attack 'unparalleled' crime. Reuters (online)

Available from: http://www.reuters.com/article/2014/12/07/us-sony-cybersecurity-probe-idUSKBN0JL00720141207

Richwine, L., 2014. Cyber attack could cost Sony studio as much as $100 million. Reuters (online)

Available from: http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209

Top Threats in 2015

Since 2011, this study has tracked challenges to business continuity worldwide by asking respondents about perceived threats according to their in-house analysis. Cyber threats are now seen as the top threat to businesses worldwide with 82% of participants stating that they are either 'extremely concerned' or 'concerned' about this. This culminates a steady climb from third in 2013 (64%) to joint second in 2014 (73%). Data from related BCI research shows cyber attacks as a long-term threat to supply chains with 54% of businesses highlighting this as a key concern[2].

Unplanned IT and telecommunications outage has been relegated to second place (81%) after topping the 2013 (66%) and 2014 (77%) Horizon Scan surveys. The difference in concern compared to cyber attacks is notable. Fewer practitioners are now 'extremely concerned' with unplanned outages (34%) as compared to cyber attacks (43%), a trend not seen since the survey began in 2012.

2. Data taken from the 2014 BCI Supply Chain Resilience Survey Report.

CASE STUDY

Ebola Virus Outbreak In West Africa

Ebola is a highly contagious, oftentimes deadly, disease which is manifested by flu-like symptoms and internal bleeding. According to the US Centers for Disease Control and Prevention (2015), the ongoing Ebola epidemic is the largest in history, causing more than 8,000 deaths and 20,000 infections over the last 10 months alone. The worst affected countries include Guinea, Liberia and Sierra Leone in West Africa. A recent World Bank (2014) report estimates that the economic cost of the outbreak may exceed US$500 billion. It is also highly likely to depress economic growth in the worst-affected countries (McKenna 2015).

References

BBC, 2014. Ebola basics: What you need to know. BBC (online)
Available from: http://www.bbc.co.uk/news/health-29556006

Centers for Disease Control and Prevention, 2015. 2014 Ebola Outbreak in West Africa. CDC (online)
Available from: http://www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/

McKenna, M., 2015. The Long Tail of Ebola: Depressing African Economic Progress. Wired (online)
Available from: http://www.wired.com/2015/01/long-tail-ebola-depressing-african-economic-progress/

United Nations, 2014. Ebola: World Bank reports economic impact in worst-hit countries to exceed $500 million in 2014. UN News Service (online)
Available from: http://www.un.org/apps/news/story.asp?NewsID=49490#.VLTwAHtHWdM

Data breach drops to third (74%) from joint second (73%) last year. Nonetheless, the percentage of respondents reporting data breach as a notable threat has increased from 65% in 2013. This reflects growing concern over financial and reputational losses caused by data breach as discussed in detail in earlier BCI reports such as 'Counting the Cost'.

Rounding out the top 10 are interruption to utility supply, supply chain disruption, security incidents, adverse weather, human illness, fire and acts of terrorism. The biggest increase in concern is observed in supply chain disruption which rose from 16th (38%) to fifth (48%) in this year's survey. This may be attributable to greater awareness of losses arising from such incidents.

Previous BCI reports reveal that 79% of organisations experience at least one supply chain incident a year[3] with almost a quarter (24%) reporting at least €1 million in losses last year[4]. Figure 2 summarises the threats as ranked by level of concern, with the percentage of respondents indicating they were 'extremely concerned' determining its final ranking.

3. Data from BCI Supply Chain Resilience Trends, 2009-2013 Surveys report
4. Data from BCI Supply Chain Resilience Report 2014

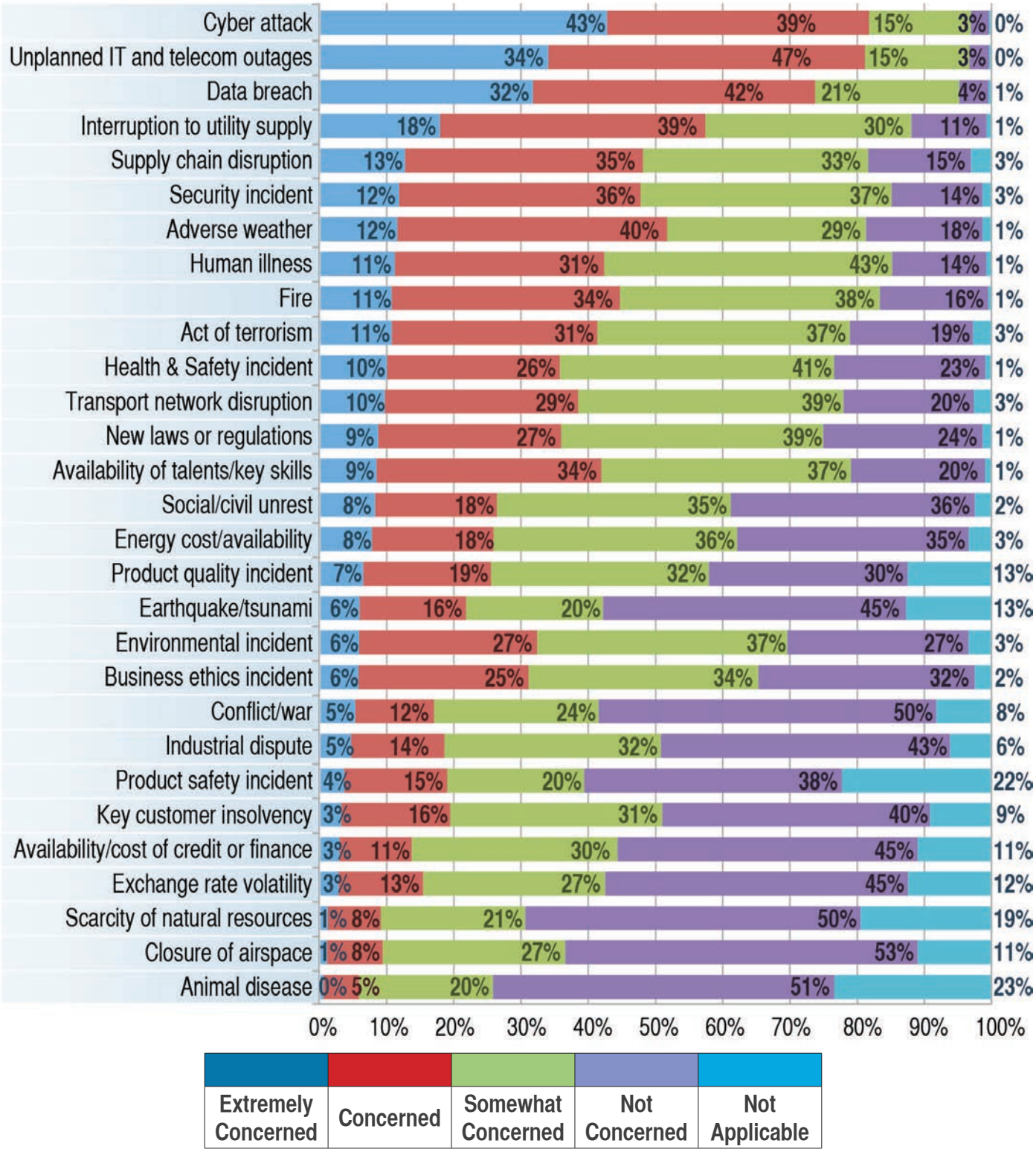


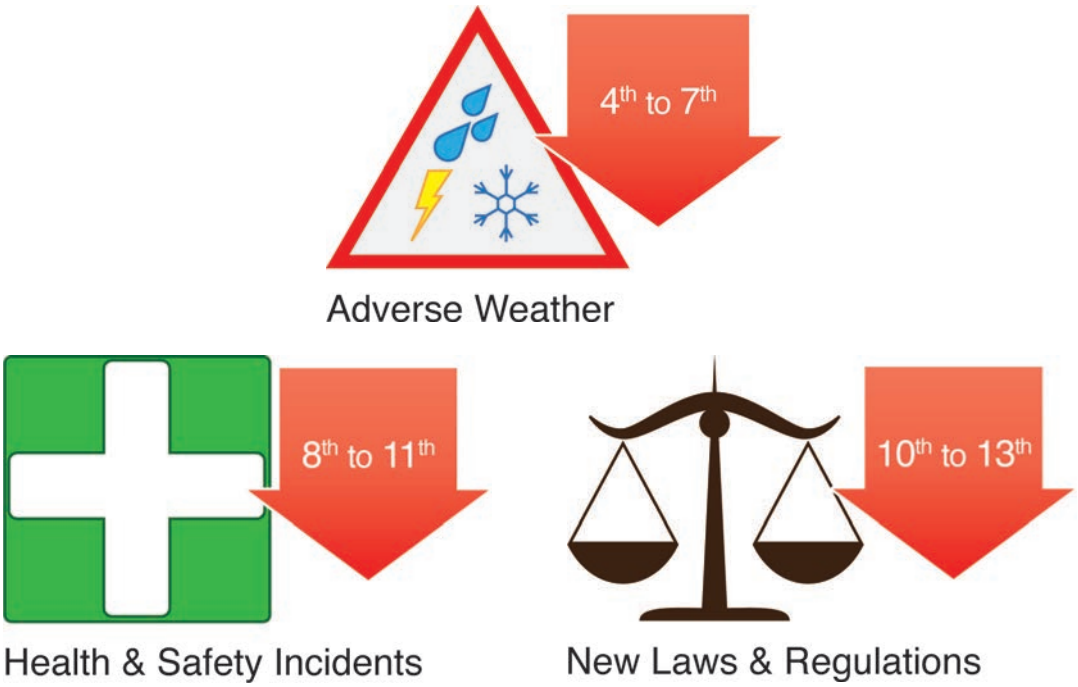
Figure 2. Question 8: Based on your analysis, how concerned are you about the following threats to your organisation in 2015? (N=694)

Figure 2 summarises the threats as ranked by level of concern, with the percentage of respondents indicating they were 'extremely concerned' determining its final ranking.

05. http://edition.cnn.com/2014/10/22/world/americas/canada-ottawa-shooting/
06. http://www.independent.co.uk/news/world/europe/charlie-hebdo-shooting-10-killed-as-shots-fired-at-satirical-magazine-headquarters-according-to-reports-9962337.html
07. http://www.economist.com/blogs/graphicdetail/2015/01/ebola-graphics

Security incidents remains firmly on the radar for practitioners as it moves to sixth from seventh in last year's survey. Meanwhile, acts of terrorism is in the top 10 for four years running. This lasting concern may perhaps be attributed to the growth of extremist groups such as the so-called Islamic State and the threat posed by returning militants. Recent terrorist activity in Sydney[5], Ottawa[6] and Paris[7] also reveal a new threat from home-grown radicals influenced by extremist propaganda.

Human illness moves into the top 10 at eighth (43%) for the first time since the survey began. This may be linked to the continuing Ebola outbreak in West Africa which has claimed almost 8,000 lives as of the end of December 2014[8]. On the other hand, adverse weather has fallen from fourth to seventh in this year's survey. Health and safety incidents (eighth to 11th) as well as new laws and regulations (10th to 13th) drop out from the top 10.



Emerging Trends and Uncertainties

The Horizon Scan also tracks in-house trend analysis performed by organisations. This year's results reveal that the top two trends remain unchanged for the third consecutive year. The use of the Internet for malicious attacks remain on top. Moreover, the proportion of participants reporting this trend have increased from 73% to 81% in 2015. This may be attributed to recent cyber attacks on organisations like Sony and the emergence of state actors perpetrating these attacks.

The influence of social media remains unchanged in second place at 63% since last year. Reflecting mounting concerns over the Ebola outbreak in West Africa, the potential emergence of a global pandemic rises to third (59%) from fifth (45%) in 2014. The erstwhile third place, new regulations and increased regulatory scrutiny, drops to fifth (53%) in this year's survey.

Rounding out the top 10 trends or uncertainties to watch out for are the loss of key employees (59%), new regulations and increased regulatory scrutiny (53%), prevalence and high adoption of Internet-dependent services (49%), increasing supply chain complexity (44%), political change (41%), changing consumer attitudes and behaviour (33%) and growing potential for social unrest (29%). Figure 3 summarises the rest of the emerging trends and uncertainties.

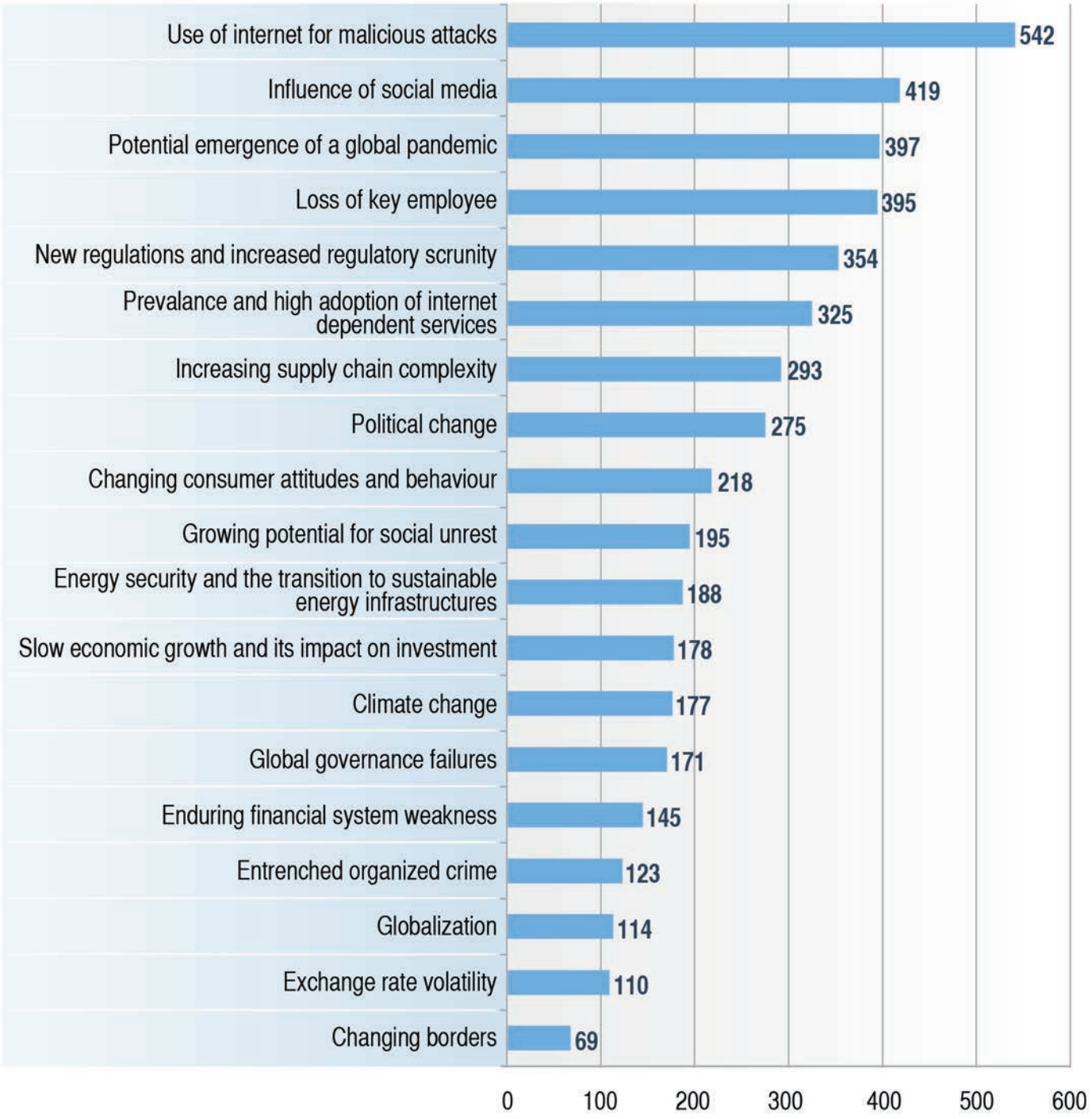


Figure 3. Question 11: Which of the following trends or uncertainties are on your radar for evaluation in terms of their business continuity implications? (N=670, multiple answers allowed)

Three trends/uncertainties drop out from the top 10 this year which are climate change (sixth to 13th), energy security and the transition to sustainable energy infrastructure (eighth to 11th), and slow economic growth (10th to 12th).

Whilst climate change has dropped out from the top 10, it may be arguable that interest in this trend may rise again over the next year given ongoing negotiations towards binding protocols limiting carbon emissions[9]. These protocols have the potential of affecting business in terms of new laws and regulations over the next few years. However, considering the steady decline in oil prices which may encourage increased consumption, this may provide a challenging backdrop to negotiations.

It is also noted that concern over slow economic growth has abated substantially in this year's survey. This may be attributed towards improving economic figures in key advanced industrial economies such as the US[10] and the UK[11]. Nonetheless, lingering economic concerns in Japan[12] and the Eurozone[13], as well as fresh turmoil in Russia[14] , may push this trend upward back into the top 10 once more.

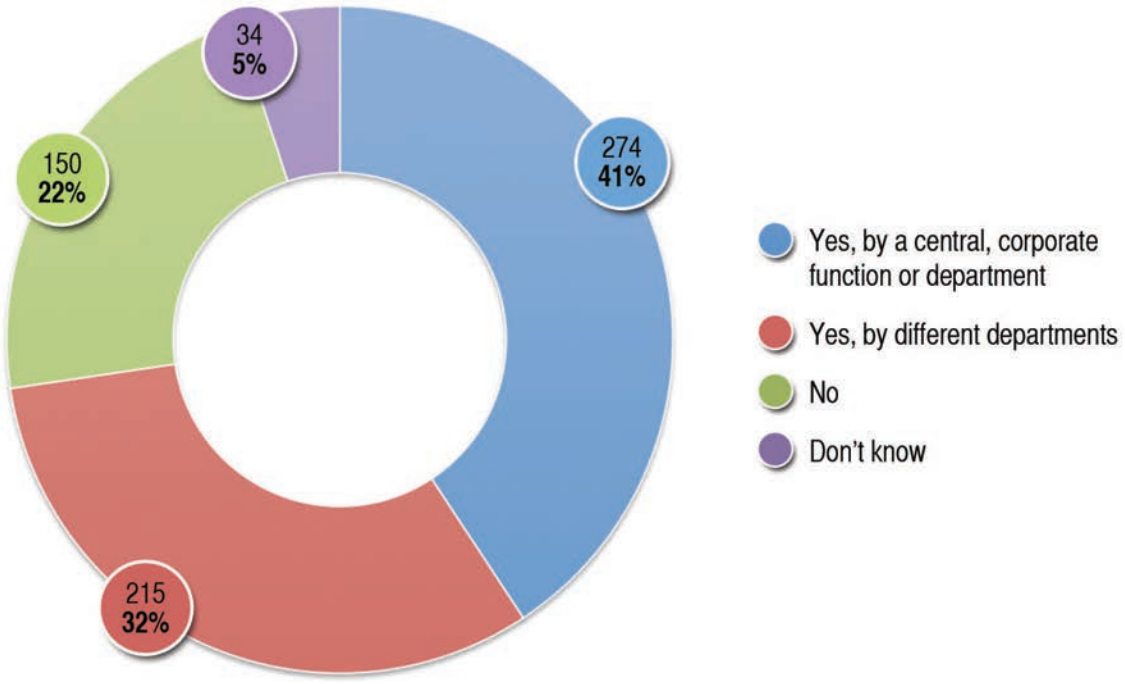


Figure 4. Question 9: Does your organisation conduct longer term trend analysis as part of its horizon scanning activity? (N=674)

The percentage of organisations employing trend analysis to better understand threats has recovered slightly from 71% in 2014 to 73% this year. More than a fifth (22%) report not employing trend analysis at all, making it a blind spot for organisations. Figure 4 summarises these figures.

09. http://www.theguardian.com/environment/2015/jan/05/paris-climate-talks-the-most-significant-task-ahead-of-us-in-2015
10. http://www.washingtonpost.com/business/economy/robust-economic-growth-in-third-quarter-raises-hopes-that-a-boom-is-on-horizon/2014/12/23/aff3a962-8adf-11e4-8ff4-fb93129c9c8b_story.html
11. http://www.theguardian.com/business/2014/oct/24/uk-economic-growth-slows
12. http://www.ibtimes.co.uk/japan-recession-deepens-gdp-growth-declines-further-1478495
13. http://www.reuters.com/article/2015/01/06/us-europe-economy-idUSKBN0KF0ZH20150106
14. http://www.wsj.com/articles/russias-economic-growth-slows-for-third-quarter-in-a-row-1415884330

Organisations in the Netherlands are more likely (82%) to utilise trend analysis whilst companies in the Middle East and North Africa (63%), Asia (65%) and Central/Latin America (67%) are less likely to do so. Segmenting the data by industry sector reveals that organisations in the health sector (48%), professional services (57%) and education (65%) are less likely to employ the method.

Nonetheless, drawing upon the outputs of trend analysis to inform an organisation's BCM programme has fallen from 53% to 43%. The proportion of companies having trend analysis and not using its input have risen from 21% to 33%. This represents a worrying figure that must be addressed by organisations as the failure to utilise trend analysis may represent another blind spot in planning and implementing a BCM programme. Figure 5 summarises the results.

The Use of In-house Trend Analysis

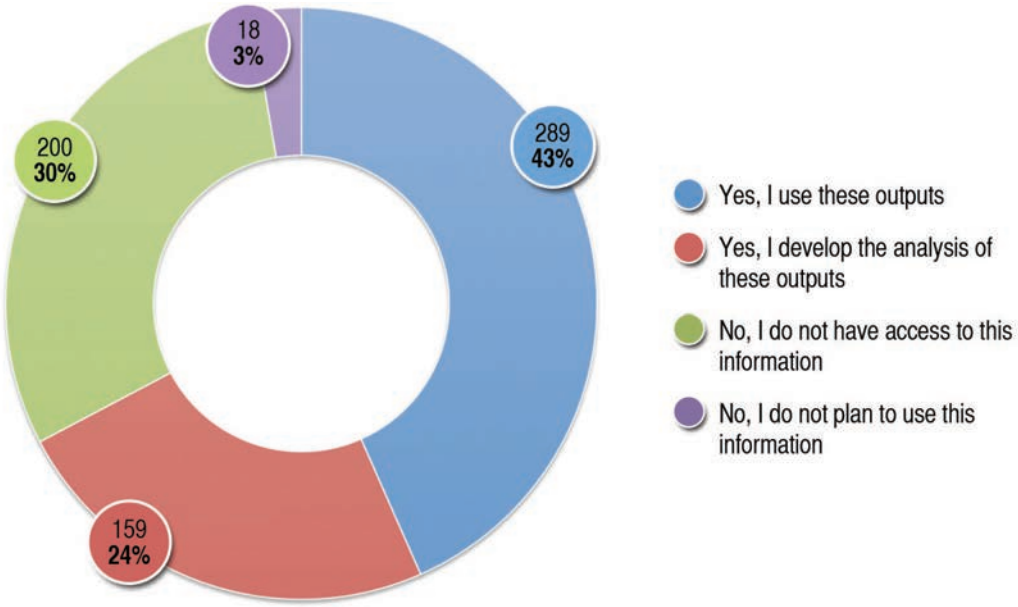


Figure 5. Question 10: As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme? (e.g. to develop scenarios or consider areas of future capability development.) (N=667)

A quick look at some responses made by survey participants captures the challenges in performing trend analysis in organisations.

- As a multi-national company, consistency in understanding and application [throughout the organisation globally] is an issue.
- Getting the business to share and communicate information on incidents and issues is difficult. In the past (1-2 years) this information has been almost non-existent… and previously the perception is that risk management/business continuity asking questions about incidents was thought to be 'meddling' by the business and was actively resisted.
- I am trying to get this in place but it is a difficult sell to top management.

Level of BC Investment

Investment for BC has increased for a greater proportion of organisations in this year's survey from 18% to 23%. Organisations in the financial/insurance (32%) and retail (45%) sectors are likely to report increased BC budgets. Companies based in Asia (32%), Sub-Saharan Africa (44%) and the Middle East (50%) are likely to report higher BC budgets as well.

For the majority of organisations, BC spending has been maintained, with 55% reporting compared to 57% last year. Organisations experiencing budget cuts have slightly increased from 11% to 12%. However, segmenting the data for industries reveal budget cuts for a significant portion of health and social care organisations (20%), public sector agencies (30%) and educational institutions (54%) which may have a negative impact on BC capabilities. Cuts are also seen for a substantial percentage of organisations in Oceania (22%) and Central/Latin America (38%). This remains a challenging condition for BC practitioners in these areas as they seek to meet growing demand for resilience amidst austerity. Figure 6 summarises the overall level of BC investment.

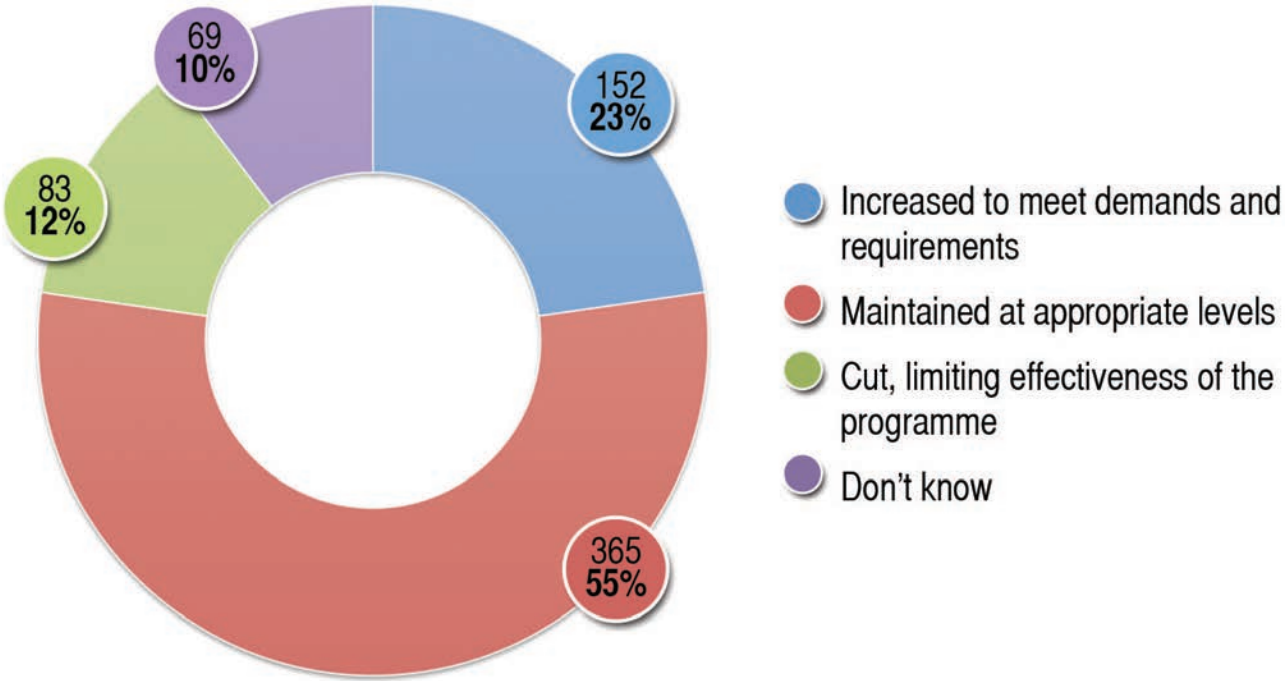


Figure 6. Question 12: If you have an existing business continuity programme, how will investment levels in 2014 compare to the current year? Investment will be... (N=670)

CASE STUDY

BCM Investment In The Middle East

A recent report by eHosting DataFort (eHDF, 2014) suggests increased BCM investment – more specifically in IT Disaster Recovery (IT DR) capability – among firms in the Middle East. Organisations reporting the presence of a dedicated BCM or IT DR team have doubled from 37% (2012) to 74% (2014). It further reveals that 27% of organisations spend US$100-250K a year to implement a BCM programme whilst 22% report spending US$250K-1 million. 11% of large organisations in the banking, oil and gas, telecoms, government and e-commerce sectors have set aside budgets of more than US$1 million.

References

eHosting DataFort, 2014. 3rd Middle East Business Continuity Management Survey. Dubai: eHDF.

The Use Of ISO 22301 As A Framework For BCM Implementation

The use of ISO 22301 as a framework for BCM implementation has increased this year, with 52% utilising the standard as compared to 44% in 2014. Organisations in the UK (61%) and Asia (64%) are more likely to report using ISO 22301 as a framework as well, mirroring the growing maturity of the standard in these areas.

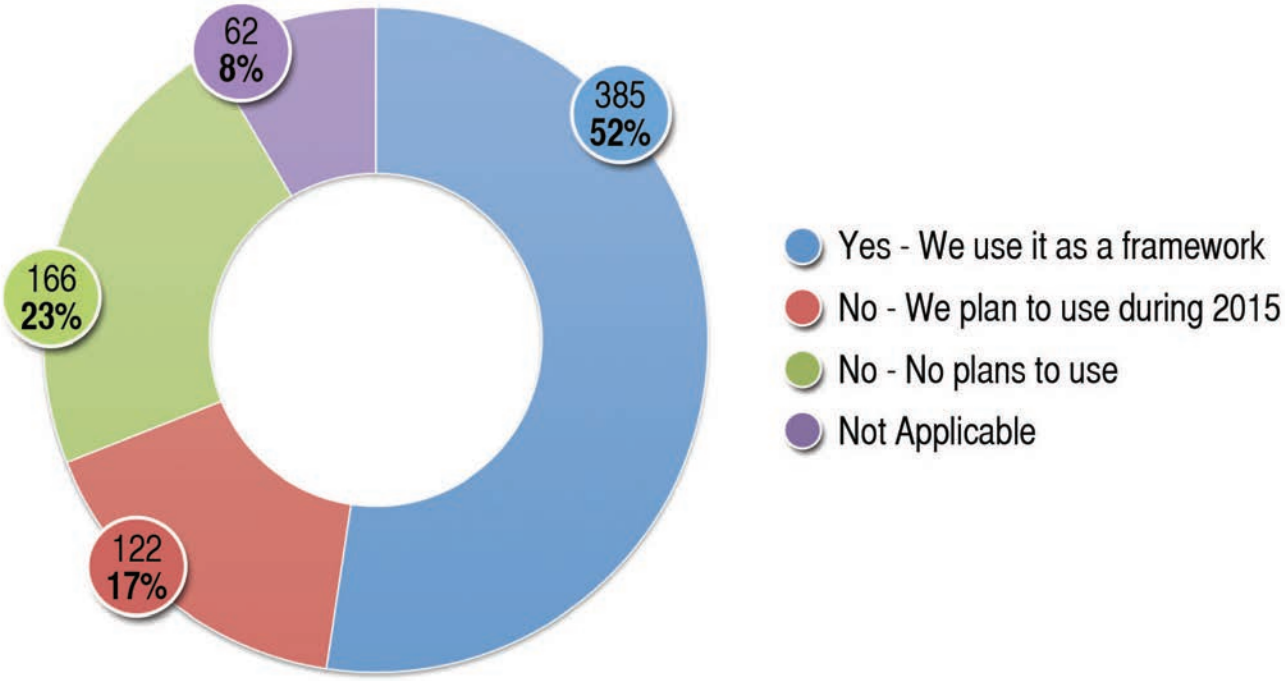


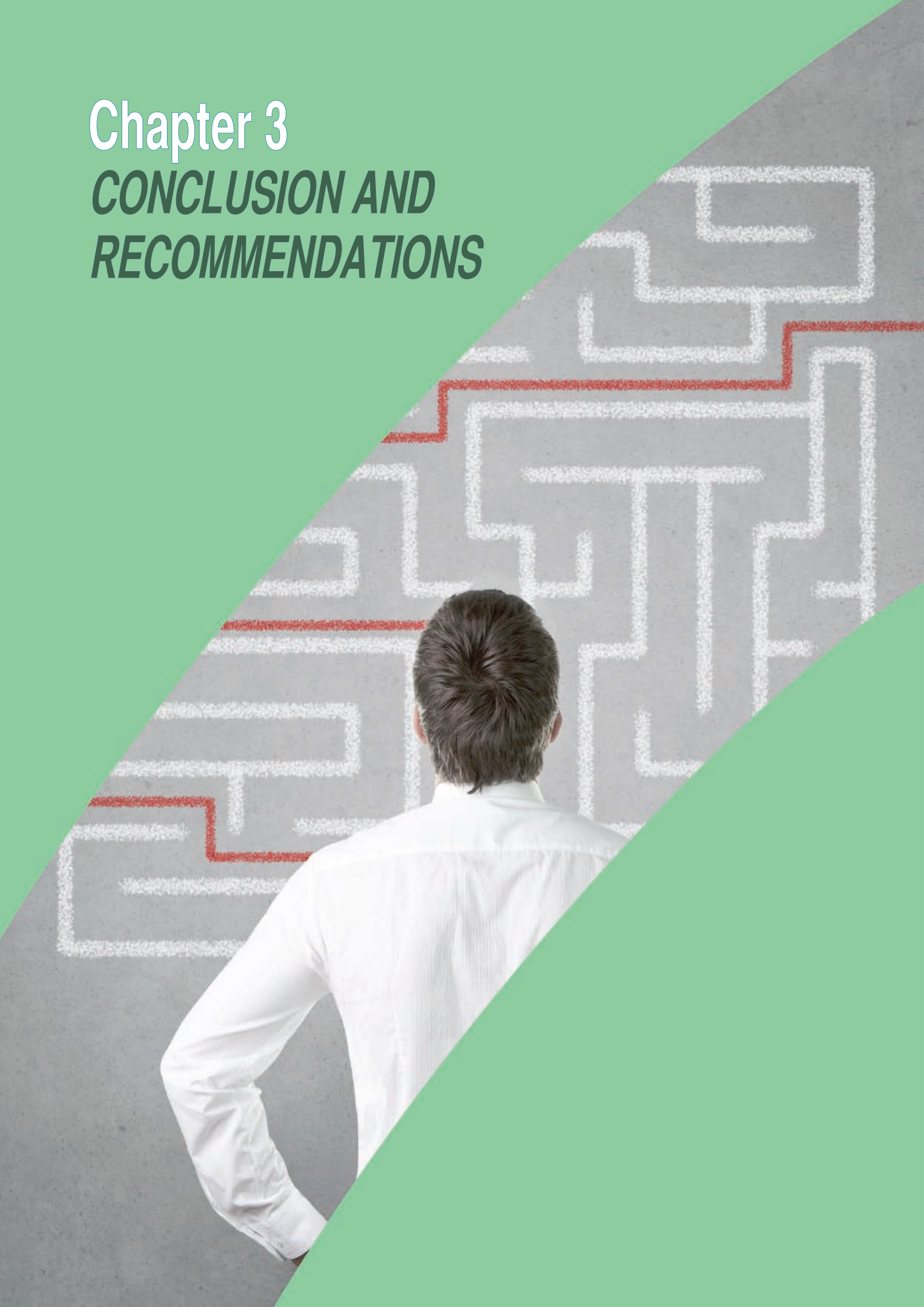
Figure 7. Question 7: If you have a formal business continuity management programme in place, how does it relate to ISO22301?

The percentage of organisations intending to use ISO 22301 this year has nonetheless decreased from 24% to 17%. Small and medium sized enterprises (50%) are also less likely to use ISO 22301 than large enterprises (53%), but it may be noticed that the gap is quite close. Figure 7 summarises the overall data on the use of ISO 22301.

This mixed picture may be attributed to the growing maturity of the standard which is reflected by the growth in the percentage of organisations aligning towards ISO 22301. Recent BCI studies support this data. According to the latest BCI Supply Chain Resilience Survey, 45% of organisations seek alignment towards a standard as a requirement for suppliers, a change from the historical average of 38%[15]. The 2013 BCI ISO 22301 Benchmarking Survey reveals that 71% of organisations are seeking to align towards ISO 22301 in the next 24 months. A lower figure of 30% is observed for certification against the standard however. These figures overall demonstrate that whilst ISO 22301 is gaining recognition as a tool to support business continuity, organisations are not yet committing to independent assessment of their systems.

15. Data from the BCI Supply Chain Resilience Survey, 2009-2013 Trends report

Chapter 3
CONCLUSION AND RECOMMENDATIONS



CONCLUSION AND RECOMMENDATIONS

The annual BCI Horizon Scan is a useful benchmarking tool for practitioners and serves to complement regular in-house analysis. It is also a good indicator of threats and uncertainties which face organisations and reflects current events. As an industry resource, the BCI Horizon Scan provides opportunities for organisations to revisit and further improve their BC planning.

This year's results affirm the mounting concern over virtual threats that negatively impact on an organisation's revenues and reputation. Cyber threats are now foremost on the radar of practitioners and notably so because of the rising costs associated with disruption. A 2014 Ponemon Institute study estimates that the average annual cost of cyber attacks worldwide is at US$7.6 million, an increase of more than 10% from the previous year[16]. A similar study by the Ponemon Institute also reveals increasing losses from data breach, with the average cost to organisations rising from US$5.4 million to US$5.9 million[17].

The threat posed by unplanned IT and telecommunications outage remains as well. Supply chain disruption mounts a strong comeback in this year's survey, with security incidents and acts of terrorism remaining as durable threats. This presents a complex threat landscape which should be accounted for in a BCM programme.

Underlying trends also round out the complex threat landscape for organisations. Uncertainties over the use of the Internet for malicious activity and the influence of social media reflect mounting concerns over virtual threats. The data suggests that BCM activity in the coming year may emanate from protecting organisations from these virtual threats.

16. Data from the 2014 Ponemon Cost of Cybercrime Report: http://www.octree.co.uk/Documents/2014-Global-Report-on-the-Cost-of-Cybercrime.pdf
17. Data from the 2014 Ponemon Cost of Data Breach Report: http://www.accudatasystems.com/assets/2014-cost-of-a-data-breach-study.pdf

The data also suggests a growing maturity of ISO 22301 with more organisations reporting their alignment to the standard and its use as a framework for BCM implementation. Nonetheless, as other BCI studies show, there are still challenges in the transition from ISO 22301 alignment to certification. This requires further exploration and should be the basis of future studies.

More organisations report employing trend analysis but there is evidence that it has less impact in influencing BCM programmes. This must be addressed as it represents wasted effort and may actually cause blind spots that negatively impact on a BCM programme's effectiveness. Given that overall levels of spending for BCM investment are increasing for a good proportion of companies, utilising trend analysis results properly may provide better value for money. This ultimately leads to a better business case on the importance of BC as a 'protective discipline' to top management. The data shows that formidable challenges exist. For one, the public sector experiences cuts in BCM investment amidst increasing demand to protect critical services. Whether this stretches public sector BC professionals to breaking point remains to be seen.

More importantly, articulating the case for business continuity as an integral 'protective discipline' towards ensuring organisational resilience remains a fundamental hurdle for many BC practitioners. BC professionals, regardless of industry sector or geographical location, face the test of justifying continued investment in BCM or resilience programmes. As such, industry resources like the BCI Horizon Scan can contribute to articulating that case.

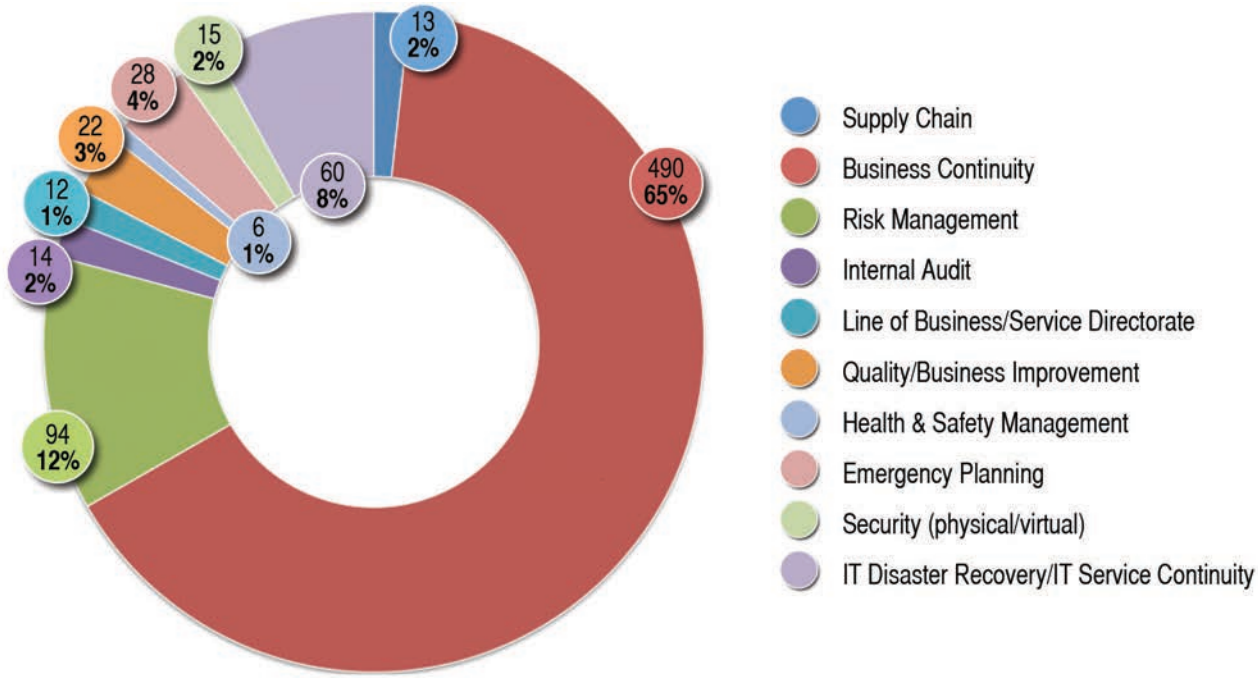
Horizon scanning is an essential activity that reveals near- and longer-term threats to an organisation. This helps maintain an organisation's viability and reputation amidst disruptive events. As such, BC practitioners can utilise insights from this activity into furthering organisational resilience.

Annex


H1 09 v H1 08
Revenue (2%)
PBT 4%
15%
4600,0
4365,0
4230,0
4222,0
4230,0
4010,0
3880,0
3758,0
3690,0
3772,2
1,665
1,844
734
540
664,5
418,0
362,0
218,6
177,1
01-Jan-09
01-Feb-09
01-Mar-09
01-Apr-09
01-May-09
01-Jun-09
01-Jul-09
01-Aug-09
01-Sep-09
01-Oct-09
01-Nov-09
Dec-09

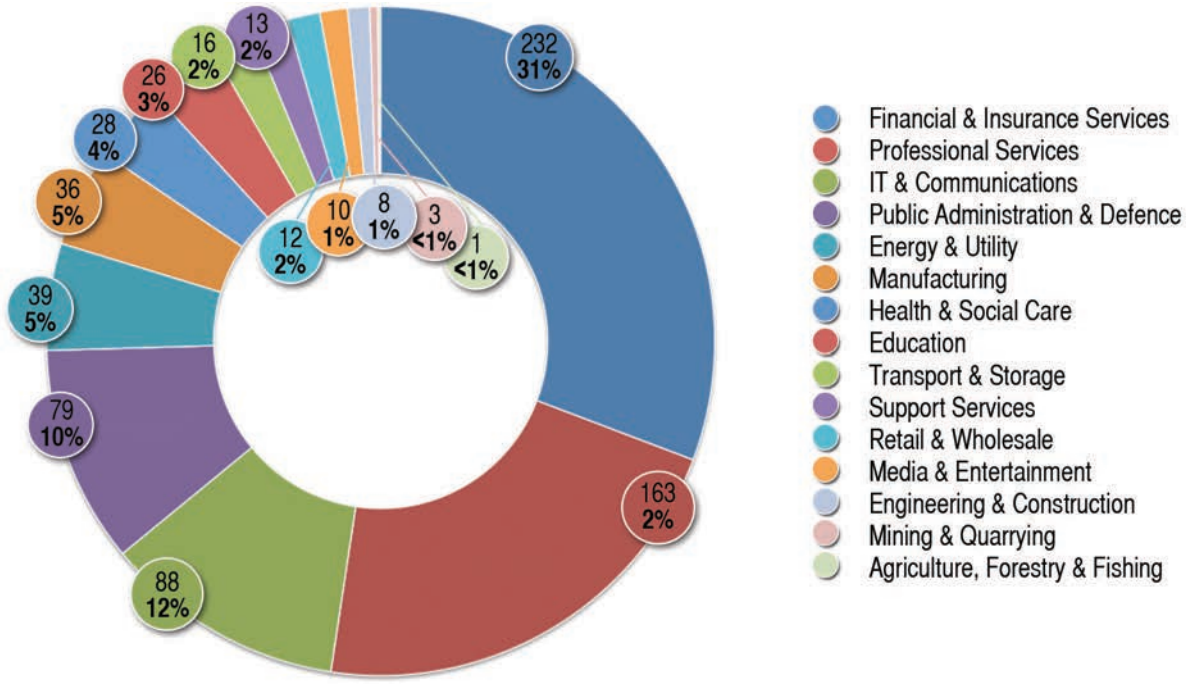
1. DEMOGRAPHIC INFORMATION

a. Functional Role of Respondents



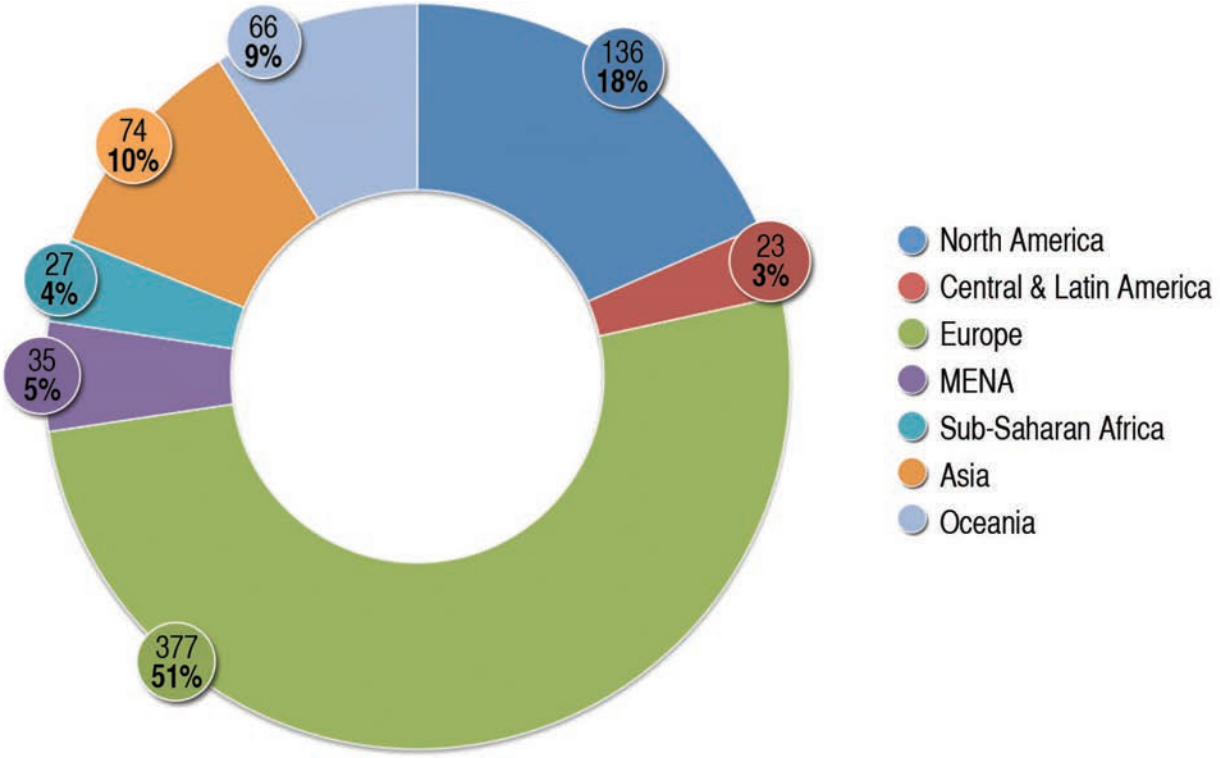
Question 1: Which of the following best describes your functional role? (N=754)

b. Industry Sector

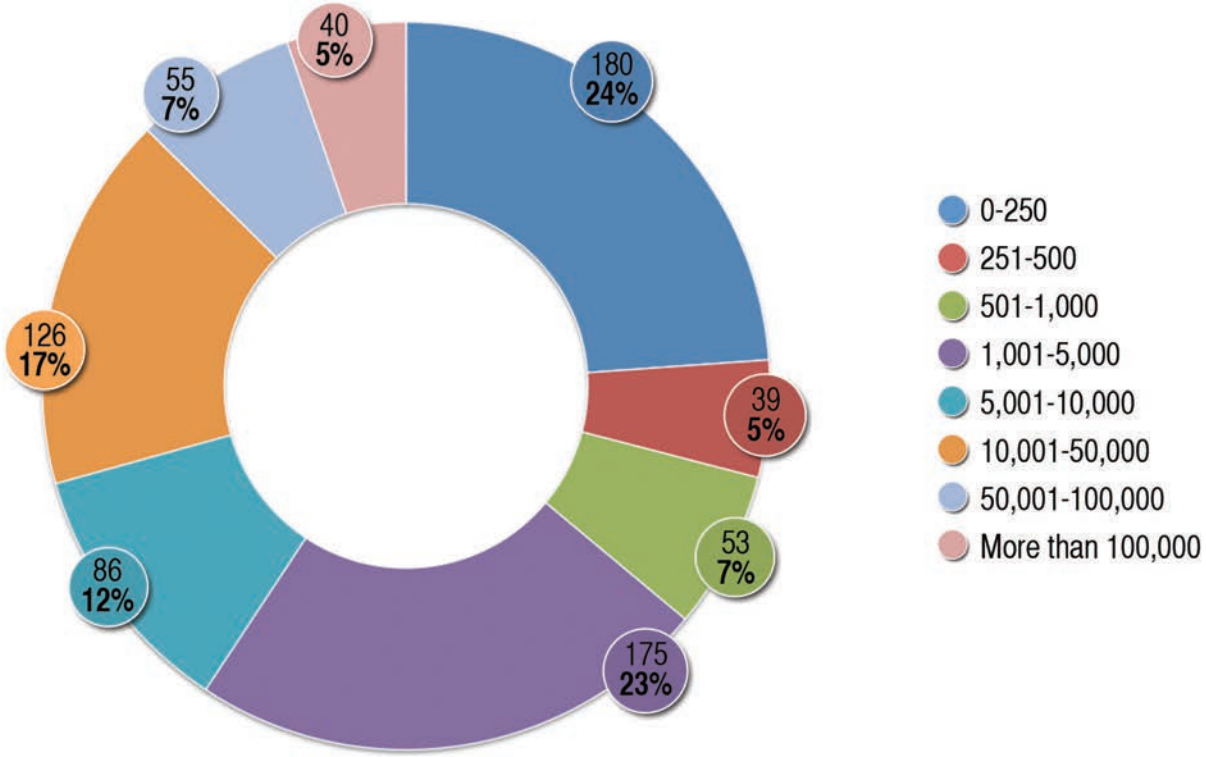


Question 2: Please indicate the primary activity of your organisation using the SIC 2007 categories given below. (N=754)

c. Geographical Base

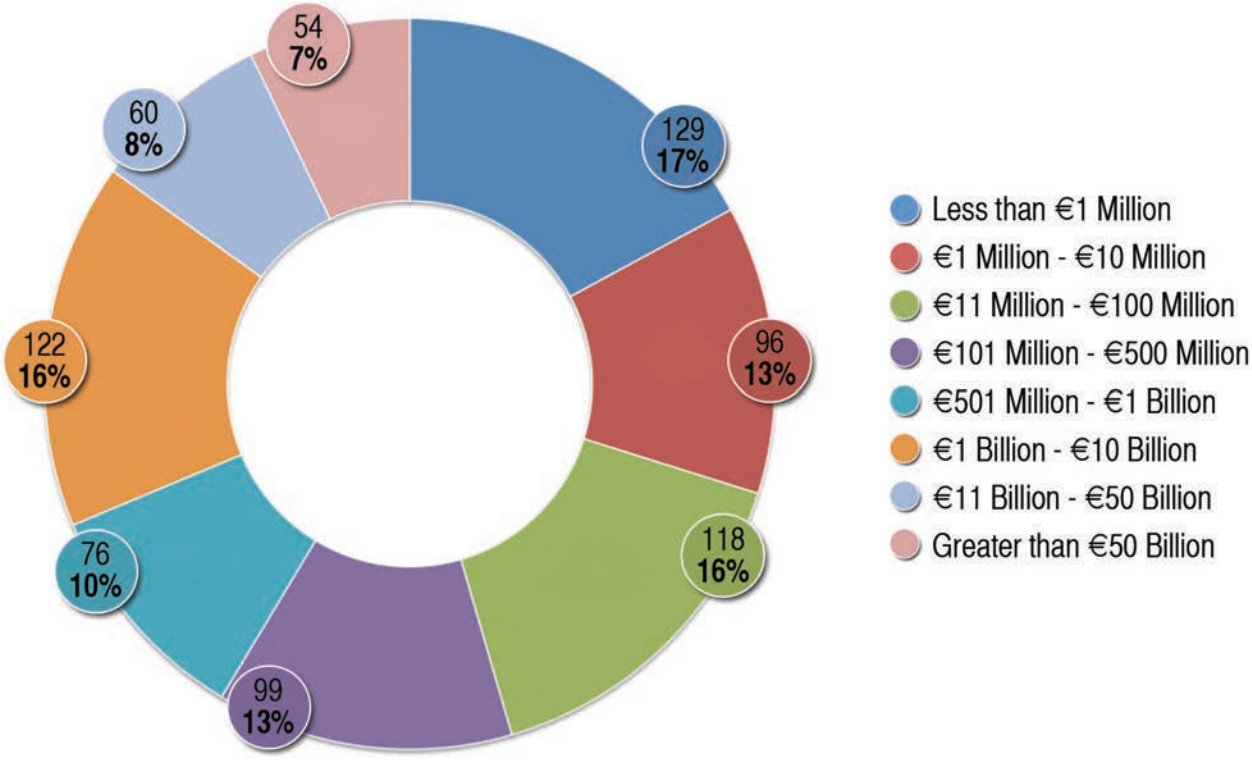


d. Number of Employees



Question 4: How many employees are there in your organisation? (N=754)

e. Approximate Annual Revenues



Question 5: What is your organisation's annual turnover? (N=754)

2. COMPARISON BY REGION/COUNTRY

	Europe	North America	Asia	Oceania
Top three threats *(Based on 'extremely concerned' responses)*	1. Cyber attack - 42% 2. Unplanned IT & telecom outages - 35% 3. Data breach - 28%	1. Cyber attack - 54% 2. Data breach - 44% 3. Unplanned IT & telecom outages - 38%	1. Cyber attack - 51% 2. Unplanned IT & telecom outages - 45% 3. Data breach - 40%	1. Data breach - 25% 2. Cyber attack - 23% 3. Unplanned IT & telecom outages - 17%
Top three trends	1. Use of Internet for malicious attacks - 82% 2. Influence of social media - 68% 3. Potential emergence of a global pandemic - 58%	1. Use of Internet for malicious attacks - 89% 2. Potential emergence of a global pandemic - 61% 3. Loss of key employee - 57%	1. Use of internet for malicious attacks - 80% 2. Loss of key employee - 68% 3. Influence of social media - 63%	1. Use of internet for malicious attacks - 76% 2. Potential emergence of a global pandemic - 61% 3. Influence of social media - 61%
Conducting Trend Analysis	73%	70%	65%	72%
Use of ISO 22301	57%	40%	64%	46%
Level Of BC Investment	Up - 21% Down - 11% Unchanged - 57%	Up - 19% Down - 12% Unchanged - 61%	Up - 32% Down - 8% Unchanged - 48%	Up - 14% Down - 22% Unchanged - 52%

	Middle East & North Africa	Central & Latin America	Sub-Saharan Africa	UK
Top three threats *(Based on 'extremely concerned' responses)*	1. Cyber attack - 50% 2. Unplanned IT & telecom outages - 41% 3. Act of terrorism - 36%	1. Cyber attack - 38% 2. Interruption to utility supply - 44% 3. Unplanned IT & telecom outages - 38%	1. Interruption to utility supply - 56% 2. Unplanned IT & telecom outages - 44% 3. Energy cost/ availability - 41%	1. Cyber attack - 39% 2. Unplanned IT & telecom outages - 35% 3. Data breach - 28%
Top three trends	1. Use of Internet for malicious attacks - 84% 2. Loss of key employee - 65% 3. Political change - 58%	1. New regulations & increased regulatory scrutiny - 71% 2. Political change - 57% 3. Increasing supply chain complexity - 52%	1. Growing potential for social unrest - 85% 2. Loss of key employee - 78% 3. Political change - 70%	1. Use of internet for malicious attacks - 81% 2. Influence of social media - 69% 3. Potential emergence of a global pandemic - 64%
Conducting Trend Analysis	63%	67%	85%	76%
Use of ISO 22301	51%	57%	63%	61%
Level Of BC Investment	Up - 50% Down - 7% Unchanged - 33%	Up - 29% Down - 34% Unchanged - 24%	Up - 44% Down - 4% Unchanged - 48%	Up - 18% Down - 14% Unchanged - 59%

2. COMPARISON BY REGION/COUNTRY

	US	Australia	Canada	Netherlands
Top three threats *(Based on 'extremely concerned' responses)*	1. Cyber attack - 55% 2. Data breach - 46% 3. Unplanned IT & telecom outages - 36%	1. Data breach - 30% 2. Cyber attack - 29% 3. Unplanned IT & telecom outages - 20%	1. Cyber attack - 48% 2. Unplanned IT & telecom outages - 41% 3. Data breach - 41%	1. Cyber attack - 48% 2. Security incident - 22% 3. Unplanned IT & telecom outages - 22%
Top three trends	1. Use of Internet for malicious attacks - 90% 2. Loss of key employee - 61% 3. Potential emergence of a global pandemic - 60%	1. Use of Internet for malicious attacks - 80% 2. Influence of social media - 64% 3. Loss of key employee - 56%	1. Use of Internet for malicious attacks - 88% 2. Potential emergence of a global pandemic - 63% 3. Influence of social media - 59%	1. Use of Internet for malicious attacks - 82% 2. Influence of social media - 70% 3. Increasing supply chain complexity - 65%
Conducting Trend Analysis	71%	71%	71%	82%
Use of ISO 22301	36%	46%	47%	29%
Level Of BC Investment	Up - 17% Down - 11% Unchanged - 63%	Up - 15% Down - 20% Unchanged - 54%	Up - 26% Down - 13% Unchanged - 58%	Up - 35% Down - 9% Unchanged - 35%

3. COMPARISON BY INDUSTRY SECTOR

	Financial & Insurance	Professional Services	Manufacturing	Public Admin & Defence
Top three threats *(Based on 'extremely concerned' responses)*	1. Cyber attack - 56% 2. Data breach - 39% 3. Unplanned IT & telecom outages - 36%	1. Cyber attack - 34% 2. Data breach - 27% 3. Unplanned IT & telecom outages - 23%	1. Unplanned IT & telecom outages - 35% 2. Supply chain disruption - 35% 3. Product quality incident - 29%	1. Unplanned IT & telecom outages - 35% 2. Cyber attack - 30% 3. Data breach - 27%
Top three trends	1. Use of Internet for malicious attacks - 87% 2. New regulations & increased regulatory scrutiny - 69% 3. Potential emergence of a global pandemic - 68%	1. Use of Internet for malicious attacks - 78% 2. Influence of social media - 64% 3. Loss of key employee - 61%	1. Increasing supply chain complexity - 77% 2. Use of Internet for malicious attacks - 68% 3. New regulations & increased regulatory scrutiny - 58%	1. Use of Internet for malicious attacks - 79% 2. Potential emergence of a global pandemic - 67% 3. Political change - 63%
Conducting Trend Analysis	78%	57%	82%	74%
Use of ISO 22301	45%	57%	56%	45%
Level Of BC Investment	Up - 32% Down - 8% Unchanged - 55%	Up - 21% Down - 8% Unchanged - 56%	Up - 19% Down - 10% Unchanged - 58%	Up - 9% Down - 30% Unchanged - 50%

	IT & Communications	Health & Social Care	Retail & Wholesale	Education
Top three threats *(Based on 'extremely concerned' responses)*	1. Cyber attack - 49% 2. Unplanned IT & telecom outages - 43% 3. Data breach - 39%	1. Data breach - 35% 2. Unplanned IT & telecom outages - 41% 3. Human illness - 27%	1. Cyber attack - 50% 2. Unplanned IT & telecom outages - 50% 3. Data breach - 33%	1. Cyber attack - 24% 2. Interruption to utility supply - 24% 3. Unplanned IT & telecom outages - 19%
Top three trends	1. Use of Internet for malicious attacks - 84% 2. Loss of key employee - 60% 3. Influence of social media - 60%	1. Potential emergence of a global pandemic - 64% 2. Use of Internet for malicious attacks - 64% 3. Loss of key employee - 56%	1. Use of Internet for malicious attacks - 82% 2. Influence of social media - 73% 3. Increasing supply chain complexity - 73%	1. Use of Internet for malicious attacks - 88% 2. Influence of social media - 77% 3. Loss of key employee - 73%
Conducting Trend Analysis	74%	48%	100%	65%
Use of ISO 22301	64%	39%	50%	54%
Level Of BC Investment	Up - 12% Down - 20% Unchanged - 48%	Up - 15% Down - 20% Unchanged - 54%	Up - 45% Down - 9% Unchanged - 45%	Up - 19% Down - 54% Unchanged - 8%

4. COMPARISON BY BUSINESS SIZE

	SMEs	Large businesses
Top three threats *(Based on 'extremely concerned' responses)*	1. Cyber attack - 30% 2. Unplanned IT & telecom outages - 24% Data breach - 24% 3. Interruption to utility supply - 19%	1. Cyber attack - 47% 2. Unplanned IT & telecom outages - 37% 3. Data breach - 34%
Top three trends	1. Use of Internet for malicious attacks - 79% 2. Loss of key employee - 67% 3. Influence of social media - 58%	1. Use of Internet for malicious attacks - 82% 2. Influence of social media - 64% 3. Potential emergence of a global pandemic - 61%
Conducting Trend Analysis	59%	77%
Use of ISO 22301	50%	53%
Level Of BC Investment	Up - 20% Down - 11% Unchanged - 56%	Up - 24% Down - 12% Unchanged - 54%

5. TRACKING TOP THREATS TO ORGANISATIONS, 2012-2015

The following indicates the percentage of respondents reporting they are 'extremely concerned' about a particular threat. Multiple answers were allowed in the survey.

Threat	2012	2013	2014	2015
Cyber Attack	24%	25%	34%	43%
Unplanned IT & Telecoms Outage	30%	28%	31%	34%
Data Breach	28%	26%	29%	32%
Interruption to Utility Supply	18%	15%	18%	18%
Supply Chain Disruption	14%	10%	9%	13%
Security Incident	N/A	12%	14%	12%
Adverse Weather	19%	14%	18%	12%
Human Illness	7%	6%	10%	11%
Act of Terrorism	13%	10%	11%	11%
Fire	16%	11%	14%	10%
Health & Safety Incident	12%	9%	13%	10%
Transport Network Disruption	11%	6%	10%	10%
New Laws & Regulations	8%	8%	10%	9%
Availability of Talents/Key Skills	9%	7%	9%	9%
Social/Civil Unrest	7%	6%	8%	8%
Energy Cost/Availability	8%	5%	7%	8%
Product Quality Incident	6%	6%	5%	7%
Earthquake/Tsunami	9%	8%	10%	6%
Environmental Incident	9%	6%	10%	6%
Business Ethics Incident	8%	8%	7%	6%
Conflict/War	5%	5%	6%	5%
Industrial Dispute	7%	4%	4%	5%
Product Safety Incident	6%	4%	5%	4%
Key Customer Insolvency	7%	4%	7%	3%
Availability/Cost of Credit	7%	6%	5%	3%
Exchange Rate Volatility	6%	4%	3%	3%
Scarcity of Natural Resources	2%	1%	3%	1%
Closure of Airspace (e.g. Ash Cloud)	2%	2%	4%	1%
Animal Disease	1%	1%	2%	1%

0-5%	6-10%	11-20%	21-30%	31-40%	>41%

Acknowledgements

The BCI wishes to thank the BSI for sponsoring this research for the fourth consecutive year. The authors also like to acknowledge the efforts of Andrew Scott CBCI during the fieldwork of this survey. Lyndon Bird FBCI provided some inputs in the writing of this report.

About the Author

Patrick Alcantara is a Research Associate for the Business Continuity Institute (BCI). In this role, he manages the delivery of the Institute's research program that focuses on global thought leadership and commercial research. His work on business continuity and resilience topics has been featured in several publications. Prior to the BCI, he has worked in the education and lifelong learning sectors. He completed a Masters in Lifelong Learning with distinction from the Institute of Education (University College London) and Deusto University under an Erasmus Mundus grant.

He can be contacted at patrick.alcantara@thebci.org.

Elliot Brooks is a Research Assistant for the Business Continuity Institute (BCI). He is finishing a degree in Disaster Management & Emergency Planning at Coventry University. His previous research work includes the 2014 BCI reports on emergency communications and supply chain resilience.

He can be contacted at elliot.brooks@thebci.org.

About the BCI

The Business Continuity Institute (BCI) is the world's leading institute for Business Continuity. Established in 1994, the BCI has established itself as the leading membership and certifying organisation for Business Continuity (BC) professionals worldwide. The BCI offers a wide range of resources for business professionals concerned with raising levels of resilience within their organisation or considering a career in business continuity.

With circa 8,000 members in more than 100 countries worldwide, working in an estimated 3,000 organisations in private, public and third sectors, the BCI truly is the world's leading institute for business continuity. The BCI stands for excellence in the business continuity profession and its membership grades provide assurance of technical and professional competency in BC.

Contact the BCI

Lyndon Bird FBCI
Technical Director

10-11 Southview Park
Marsack Street
Caversham RG4 5AF
United Kingdom

+44 (0) 118 947 8215
lyndon.bird@thebci.org

Business Continuity Institute

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 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 intvernational 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, Automotive, Built Environment, Food, Healthcare and ICT. With over 80,000 clients in 172 countries, BSI is an organisation whose standards inspire excellence across the globe.

To learn more, please visit www.bsigroup.com.

Contact BSI

Nigel McGimpsey
Business Development Director

Kitemark Court
Davy Avenue
Knowlhill, Milton Keynes
MK5 8PP
United Kingdom

+44 (0) 84 5080 9000
nigel.mcgimpsey@bsigroup.com

bsi.

Business Continuity Institute

10-11 Southview Park
Marsack Street
Caversham
RG4 5AF
United Kingdom

+44 (0)118 947 8215
www.thebci.org

Correct at February 2015