Business Continuity Institute

HORIZON SCAN REPORT 2016

Business Continuity Institute

bsi.

BCI Foreword

David James Brown FBCI
BCI Chairman

I am proud to present the fifth Horizon Scan survey report as a result of the collaboration between the Business Continuity Institute and BSI. As the Chairman of the BCI, I would also like to compliment our research team for their efforts and dedication.

In 2015 we have seen old and new types of risk materialise to test societies around the world. Online threats are confirmed as the main challenge for businesses, due to their increased sophistication and consequences. Physical security is a renewed priority, due to the increase in terror attacks across many countries. Climate change has heightened the risks of disruptions caused by adverse weather, sea level rise and unprecedented periods of drought. It is because of the diversity and potential impact of these events that I believe this piece of research to be one of the most significant the BCI has ever published.

The need perceived by organizations to identify and build resilience to this range of threats reveals the importance of this survey for business continuity professionals, the Horizon Scan's reputation and reliability make it one of the most popular reports in the industry on a global scale. It is indeed crucial for practitioners to advise organizations on what to prepare for and adjust their recovery plans accordingly.

The industry landscape is rapidly changing, and so should our discipline in order to keep up with both traditional and modern challenges. At the top of the list this year as expected we continue to see threats such as cyber-attack, data breach and unplanned IT outages. The TalkTalk incident in the UK, the Great Cyber Bank Heist and the outage to the New York Stock Exchange are all examples that organizations must sit up and take notice of.

More traditional threats such as terrorism continue to be 'front-of-mind' for organizations. Given the rise of new challenges and the fact that old ones remain, horizon scanning techniques are even more valuable in assisting organizations to be prepared to the best of their potential.

BSI Foreword

Howard Kerr
BSI Chief Executive

The results of this, our fifth report with the BCI, reflect the stark realities of the world in which we live today. The business environment is ever more dynamic, and we operate in the face of the mounting challenges that brings. This requires organizations to shift their thinking, and adapt to the risks and the opportunities if they are to survive and thrive. To ensure lasting success, an organization must become 'resilient'; finding opportunity in the face of challenge. At BSI we call this ability Organizational Resilience.

Cyber attacks remain the primary challenge to information gathering and sharing according to the views of those we polled. Meanwhile the potential risk of data breaches - and their much-publicised fall-out - has become more prevalent, rising to become the second biggest perceived threat. In today's digital world, individual and business customers must be able to trust companies to be run securely and to have adequate protocols in place to protect their sensitive data. So, a resilient organization must gather, use and store information appropriately to protect itself against these threats in the short and long-term.

Information resilience is just one of the three domains across which organizations must display resilience. Organizations must be similarly vigilant and adaptable across their operations and supply chain. The findings of this report reflect this, with concerns in the top 10 spanning these areas.

Acts of terrorism are now the fourth biggest cause for concern, up from 10th just a year ago. And with the effect of weather patterns like El Nino affecting local communities with greater frequency, it is small wonder that adverse weather remains in the top 10. As organizations become increasingly reliant on complex supply chain networks spanning continents, it is encouraging to see that the major causes of supply chain disruption are taken so seriously.

Despite this awareness of risk, it is concerning to see that a quarter of all organizations still do not run any kind of long-term trend analysis at all. A third do not make use of the results to assess and better understand threats. Of some comfort, half of those surveyed for this report have embraced ISO 22301 as a framework for business continuity management.

It is difficult to conceive that either investors or employees will be reassured that the leaders of the organizations they trust are making strategic decisions without an effective evaluation of risk.

Ultimately, organizations must recognize that, while there is risk, and plenty of it, there is opportunity. Taking advantage of this means that leaders can steer their businesses to succeed by not just surviving, but thriving.

For us, Organizational Resilience is positive and forward-thinking; it allows management to take calculated risks with confidence, seize new opportunities with enthusiasm, protect their license to operate with credibility, boost their business credentials and, ultimately, enhance their reputation.

The findings of the report show that Organizational Resilience is now a strategic imperative for all companies, big and small. That means making excellence a habit - across the business, from products and services to people and processes, and from vision and values to culture and behaviours. And it demands agile leadership, strategic adaptability and robust governance.

One thing is clear: the ability of an organization to anticipate, prepare for, respond to and adapt to change and crucially to prosper from it - is more important now than ever. A resilient organization is one that not merely survives over the long term, but also flourishes - passing the test of time.

Contents

1 | Executive Summary

BCI Horizon Scan 2016

568 responding organizations

74 countries

Top 10 Threats

1st Cyber attack

2nd Data breach

3rd Unplanned IT & telecom outages

4th Act of terrorism

5th Security incident

6th Interruption to utility supply

7th Supply chain disruption

8th Adverse weather

9th Availability of talents / key skills

10th Health & safety incident

Top 5 Trends and Uncertainties

1st Use of Internet for malicious attacks

2nd Influence of social media

3rd Loss of key employee

4th New regulations & increased regulatory scrutiny

5th Prevalence & high adoption of internet - dependent services

Trend Analysis

26% of organizations do not perform longer-term trend analysis

33% of organizations DO NOT use trend analysis results

58% SMEs are less likely to perform trend analysis than large businesses (74%)

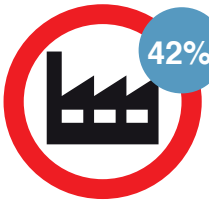
ISO 22301 Uptake

24% of organizations are likely to increase BC spend in 2016

11% of organizations will cut BC budgets in 2016

37% of MENA-based organizations are increasing BC spend

Increased investment seen in



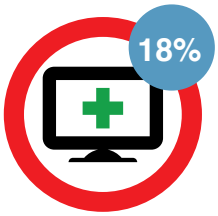
Manufacturing

Retail

IT/ telecommunications

Budget cuts expected in

Education



Health & social care

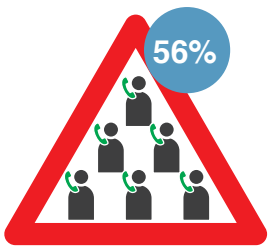
Public administration

Investment in Business Continuity

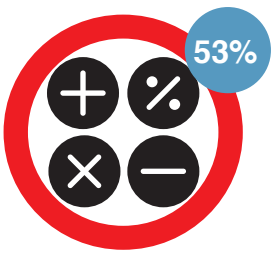
51% of organizations claim using ISO 22301 as a framework for business continuity management

Highest uptake of ISO 22301 seen in

IT/ telecommunications



Professional services



Financial

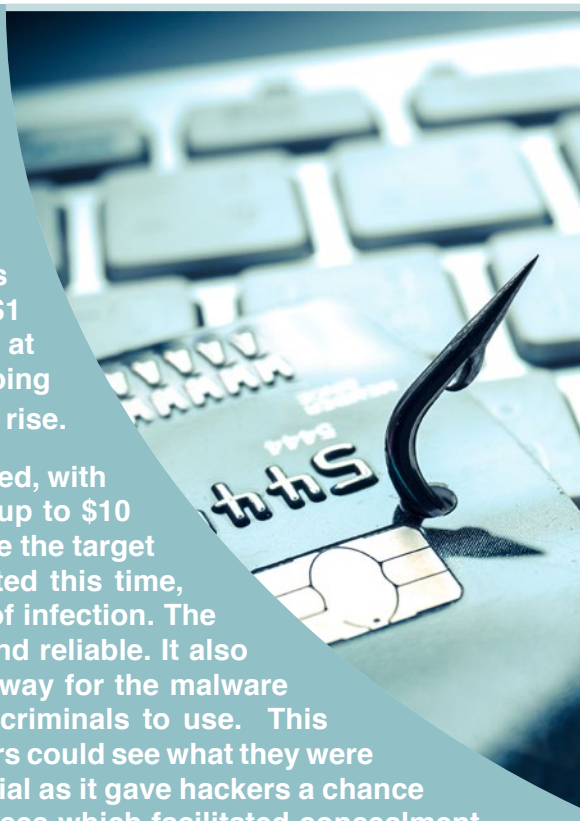
2 | Horizon Scan Report 2016

In association with BSI, the BCI Horizon Scan Report is an annual exercise that seeks to identify near-term threats to organizations worldwide. It also measures the sentiment of business continuity (BC) and resilience professionals by indicating their level of concern to different risks and threats. As a respected industry resource, the report complements in-house analysis and benchmarks horizon scanning activity among organizations across regions and industry sectors. Data cited in this report was obtained from a survey which began on October 2015 and ran for eight weeks. 568 organizations from 74 countries participated in this study.

On its fifth edition, the BCI Horizon Scan Report tracks risks and threats to organizations through assessing perceived threats as shown by practitioners' in-house analysis. Cyber attacks such as malware and denial of service retain the top position with 85% of respondents[1] stating being 'extremely concerned' or 'concerned' about this threat. This coincides with findings from other BCI research showing cyber attacks as the top long-term threat to supply chains (46%)[2]. Cyber attacks and related cyber security incidents are also one of the top 10 triggers for activating emergency communications plans (28%)[3].

Data breach rises to second (80%) from third (74%) in 2015. Organizations indicating they are 'extremely concerned' about this threat materialising have increased from 32% to 41% this year. Meanwhile, unplanned IT and telecommunications outages drops from second (81%) in 2015 to third (77%) this year.

Case Study:
The Great Cyber Bank Heist



In February 2015, a joint effort by Interpol, Europol, and Kaspersky Lab (a cybersecurity company) revealed what is thought to be the largest bank theft of all time. A gang of cybercriminals named Carbanak breached the defence systems of over 100 banks around the world, stealing an estimated $1 billion through a series of hackings. While confirmed losses at the moment is set at $300 million, the investigation is still ongoing and the group is still active. As such, figures are very likely to rise.

The attacks went on for over two years before being detected, with each intrusion lasting for 2-4 months, costing organizations up to $10 million[4]. Spear phishing was used by the attackers to penetrate the target banks' internal networks. Staff members were directly targeted this time, unlike previous instances when end users became the point of infection. The email used by the attackers was well-crafted to look formal and reliable. It also included a word document that once downloaded paved the way for the malware which contained a remote administration tool (RAT) for the criminals to use. This allowed access to the banks' computers to the point that hackers could see what they were doing by gaining access to surveillance cameras[5]. This is crucial as it gave hackers a chance to see credentials, habits and working patterns of the employees which facilitated concealment of their illegal acts. Stolen money was then either transferred through simple e-banking ways or collected by accomplices in compromised ATM machines which responded to the hackers' commands[6]. This case suggests that banks might want to redouble their efforts and provide an industry-wide response given that hackers are likely to keep using the SWIFT (funds transfer) and ATM (cash disbursement) systems in their operations[7].

1. The figure cited is a total of participants indicating they are either 'extremely concerned' or 'concerned' over a specific threat unless indicated otherwise.

2. Data taken from the 2015 BCI Supply Chain Resilience Report

3. Data taken from the 2015 BCI Emergency Communications Report

4. http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab

5. http://www.ibtimes.co.uk/billion-dollar-bank-job-how-hackers-stole-1bn-100-banks-30-countries-1488148

6. http://finance.yahoo.com/news/great-bank-robbery-carbanak-cybergang-191800014.html

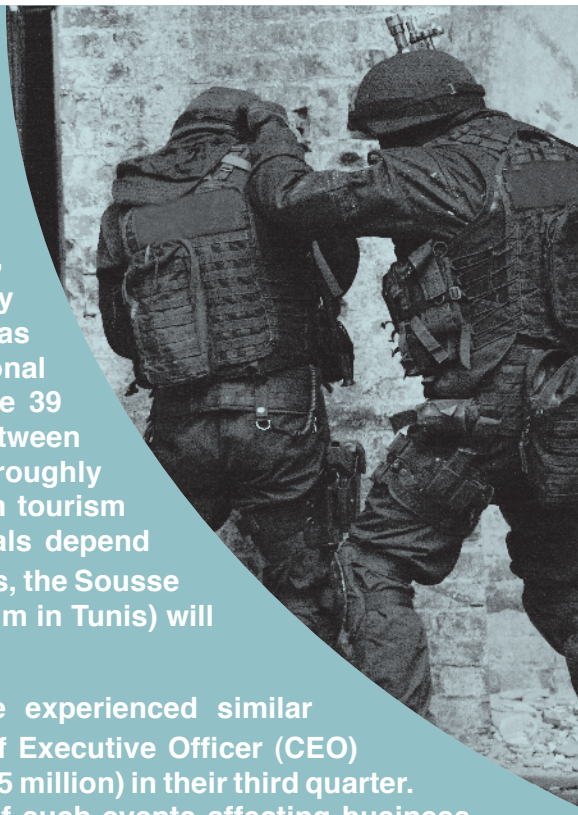
7. https://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts/

Acts of terrorism jump six places from tenth (42%) to fourth (55%), with 19% of respondents stating they are 'extremely concerned'. This may be attributed to the recent spate of terrorist attacks in Paris and other parts of the world which occurred during the survey period. This result shows how current events can influence the perception of risks and threats.

Rounding out the top 10 are the following threats: security incident (fifth), interruption to utility supply (sixth), supply chain disruption (seventh), adverse weather (eighth), availability of talents/key skills (ninth) and health and safety incident (tenth). Security incidents rank higher this year at fifth compared to sixth last year. 17% express that that they are 'extremely concerned' about this threat from 12% in 2015.

Supply chain disruptions are in the top 10 for second year running at seventh. Findings from other BCI studies confirm that this remains costly for many organizations with 9% of organizations losing at least €1 million as a result of single incident[8]. 56% of organizations claim that these losses are entirely uninsured[9]. Another BCI study focusing on the retail industry reveals that 18% of organizations in the sector invoked their BC plans in the last 12 months due to this type of incident[10].

Case Study: Tunisia Terror Attacks



In June 2015, a gunman with links to religious extremists opened fire on the Tunisian beach of Sousse and killed 39 people. All of the victims came from western countries, including 30 British citizens[11]. The attack disrupted everyday life and tourism in the North African country as well as companies operating in the area. The TUI Group, a multinational travel company, suffered a considerable hit as 33 out of the 39 victims had flown to Tunisia with a TUI holiday package. Between travel cancellations and repatriation costs, the company lost roughly €40 million, a setback that also impacted the fragile Tunisian tourism industry which includes local shops and markets many locals depend on[12]. With Tunisian tourism experiencing growth in recent times, the Sousse attack (coupled with the earlier terror incident at Bardo Museum in Tunis) will likely have a negative impact on the sector.

TUI's case is mirrored by other companies who have experienced similar difficulties promoting travel to Tunisia[13]. However TUI's Chief Executive Officer (CEO) underlined how the company still registered profits (roughly £35 million) in their third quarter. It was revealed how TUI regularly considers the possibility of such events affecting business and prepares accordingly[14]. This shows the importance of horizon scanning and trend analysis especially in the light of increased security concerns worldwide.

8. Data taken from the 2015 BCI Supply Chain Resilience Report
9. ibid.
10. Data taken from the 2015 BCI Global Retail Resilience Report
11. http://www.reuters.com/article/us-tunisia-security-idUSKBN0P61F020150628#TcREj9JTIFFZoZA3.97
12. http://www.theguardian.com/business/2015/aug/13/tunisian-attacks-dominate-tui-travel-results
13. http://edition.cnn.com/2015/06/26/travel/tunisia-terror-sousse-tourism/index.html
14. http://uk.businessinsider.com/tui-and-thomas-cook-results-tunisia-tragedy-will-hit-companies-2015-8?op=1

Availability of talents/key skills makes a comeback in the top 10 at ninth. Health and safety incidents rise one place from 11th to tenth. This coincides with the increase in organizations invoking emergency communications plans to deal with this type of incident (17% to 32%)[15]. Fire drops out of the top 10, finishing at 11th (10% extremely concerned). Human illness also exits the top 10 from eighth last year.

As shown on the following page, Figure 1 summarises the threats as ranked by level of concern. Segmented data for selected industry sectors and regions are available in the Annex of this report.

15. The comparison was made from the 2014 and 2015 editions of the BCI Emergency Communications Report.

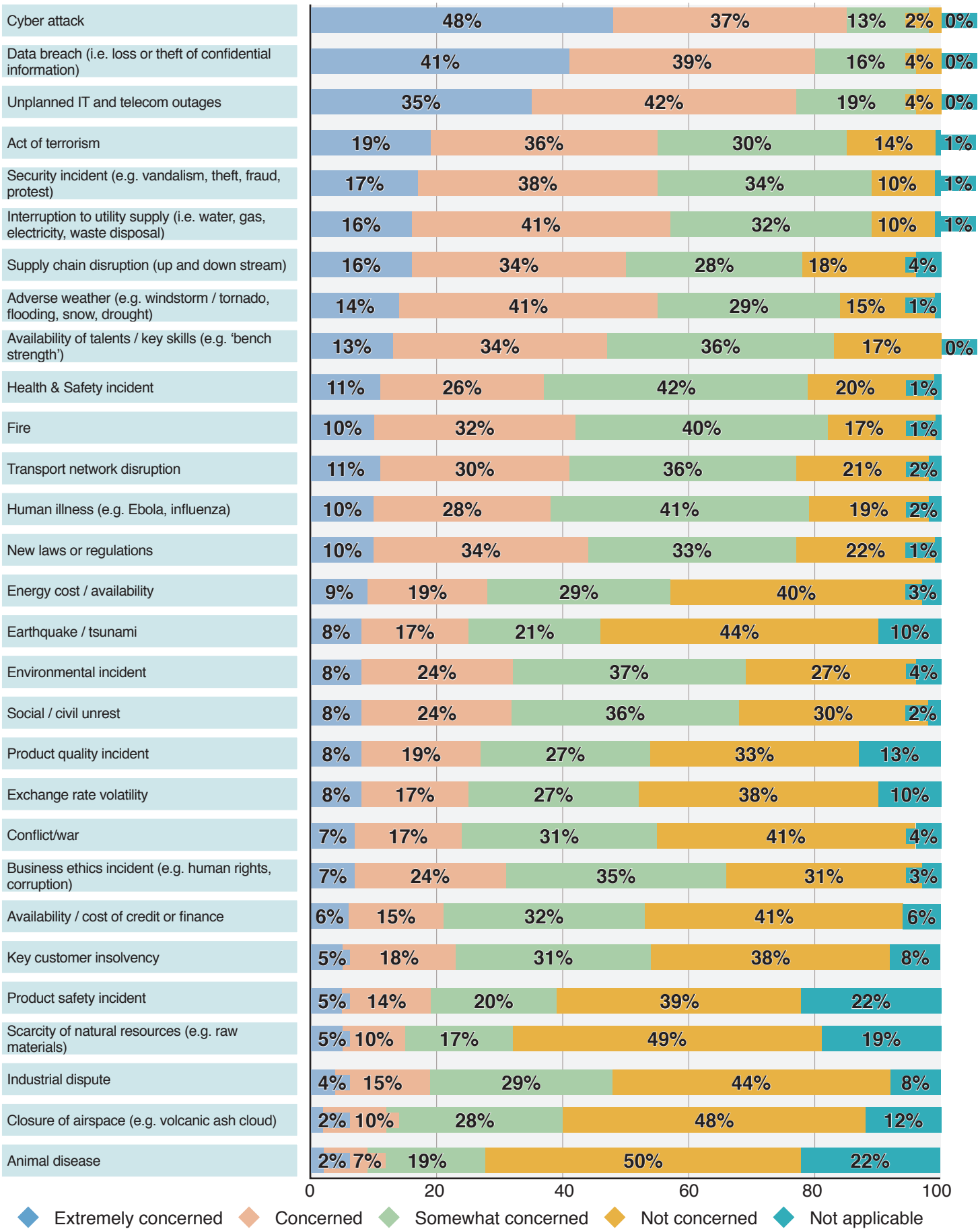


Figure 1. Question 7: Based on your analysis, how concerned are you about the following threats to your organization in 2016? (Numbers are expressed as percentage, N=511)

Emerging Trends and Uncertainties

Measuring practitioner sentiment for specific business trends and uncertainties also feature in the Horizon Scan analysis. The increasing use of the internet for malicious attacks remains on top once again as practitioners indicate their increased concern over cyber attacks, data breach and other related incidents. The proportion of respondents following this trend has increased slightly from 81% in 2015 to 83% this year.

The growing influence of social media especially in relation to company reputation is placed second in this year's report with 63% of respondents concurring. The loss of a key employee now rises from fourth last year to third place (56%). The likelihood of new regulations and increased regulatory scrutiny is more closely monitored this year with 55% of respondents indicating this in their trend analyses. The prevalence and high adoption of internet dependent services such as cloud-based solutions increases one place to fifth (50%). The rise of a global pandemic, ranked third last year (59%), drops to sixth (48%).

Rounding out the top 10 are increasing supply chain complexity (47%), political change (42%), changing consumer attitudes and behaviour (36%) and energy security/transition to sustainable energy infrastructures, climate change and social unrest (29%). Figure 2 summarises the data. The Annex contains segmented data according to industry sector and region.

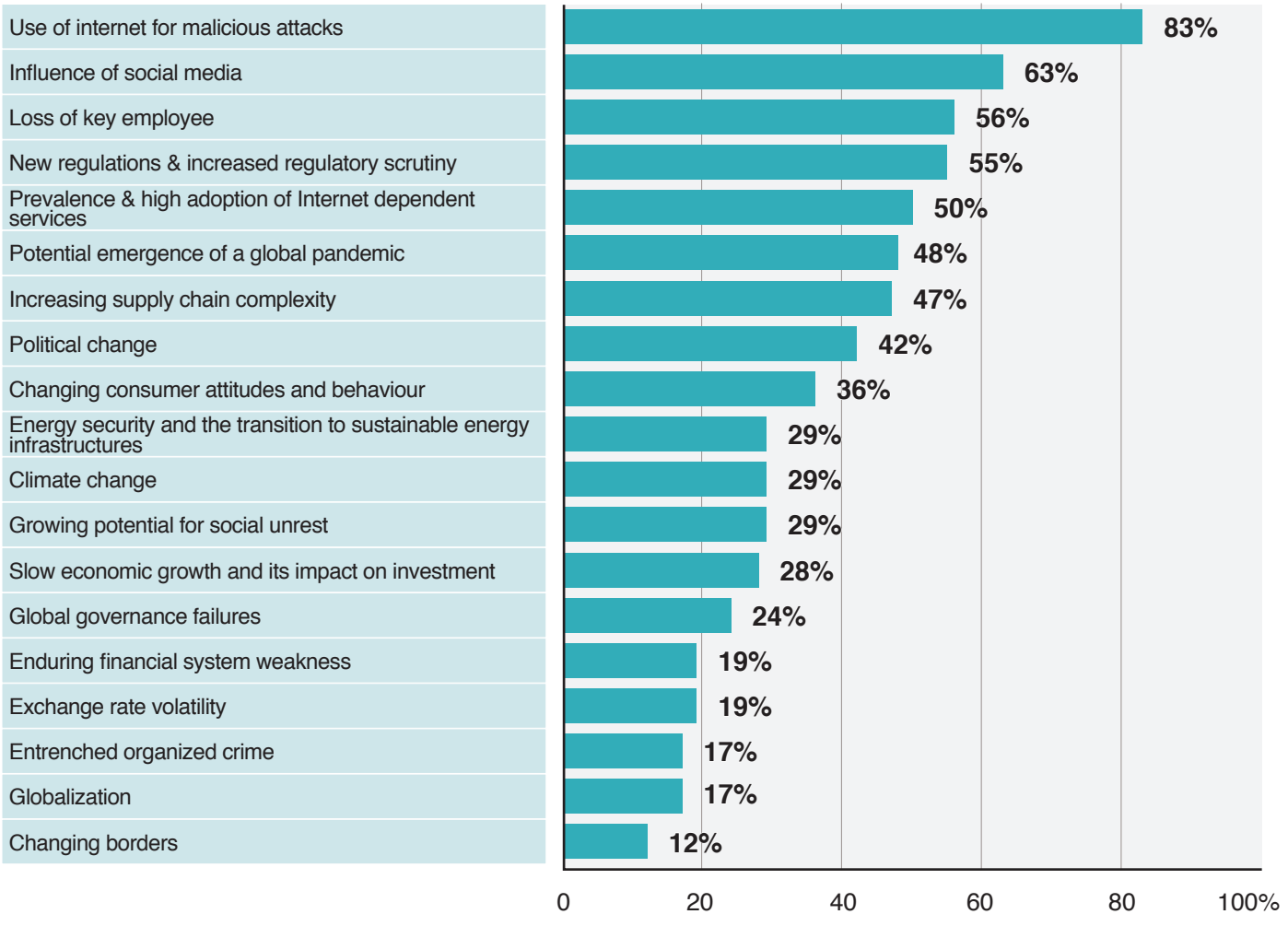


Figure 2. Question 10: Which of the following trends or uncertainties are on your radar for evaluation in terms of their business continuity implications? (Answers are expressed as percentage, N=497)

Benchmarking Longer-term Trend Analysis

70% of organizations perform longer-term analysis to assess and better understand threats, a slight decline from 73% last year. More than a quarter of organizations (26%) do not engage in this exercise at all which is a worrying figure. Figure 3 summarises the data.

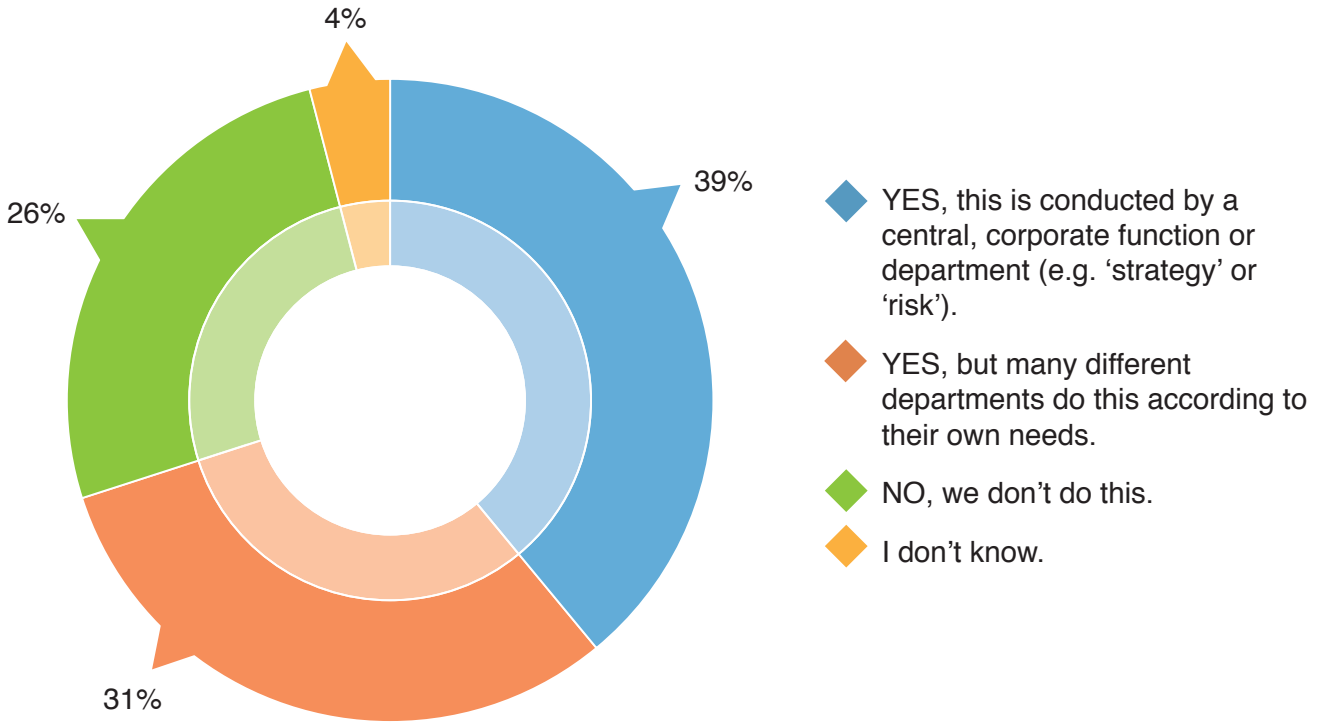


Figure 3. Question 8: Does your organization conduct longer term trend analysis as part of its horizon scanning activity? (Numbers are expressed as percentage, N=496)

Large businesses are more likely to engage in longer-term trend analysis than small and medium sized enterprises (SMEs) at 74% to 58%. Data segmented according to industry sectors reveal that the top three industries performing trend analysis are the following: public administration and defence (86%), finance (76%) and education (65%). Among regions, the highest rates of trend analysis are observed in Oceania (75%), Asia (75%) and Europe (72%). Among countries which returned at least 2.5% to the total respondent count[16], the following report the highest figures: Canada (94%), Netherlands (86%) and Australia (78%).

16. These countries include the United Kingdom (UK), United States (US), Australia, New Zealand, Canada, Netherlands and South Africa.

Measuring the use of trend analysis in informing BCM implementation, 33% reveal not using its results (Figure 4). This statistic remains unchanged from last year. SMEs outperform large businesses in this area, with 71% using trend analysis results in their BCM programmes as opposed to 66%. Looking across industry sectors reveal that organizations in the public sector (78%), professional services (76%) and finance (70%) surpass the average. The same is also observed with organizations based in Europe (69%).

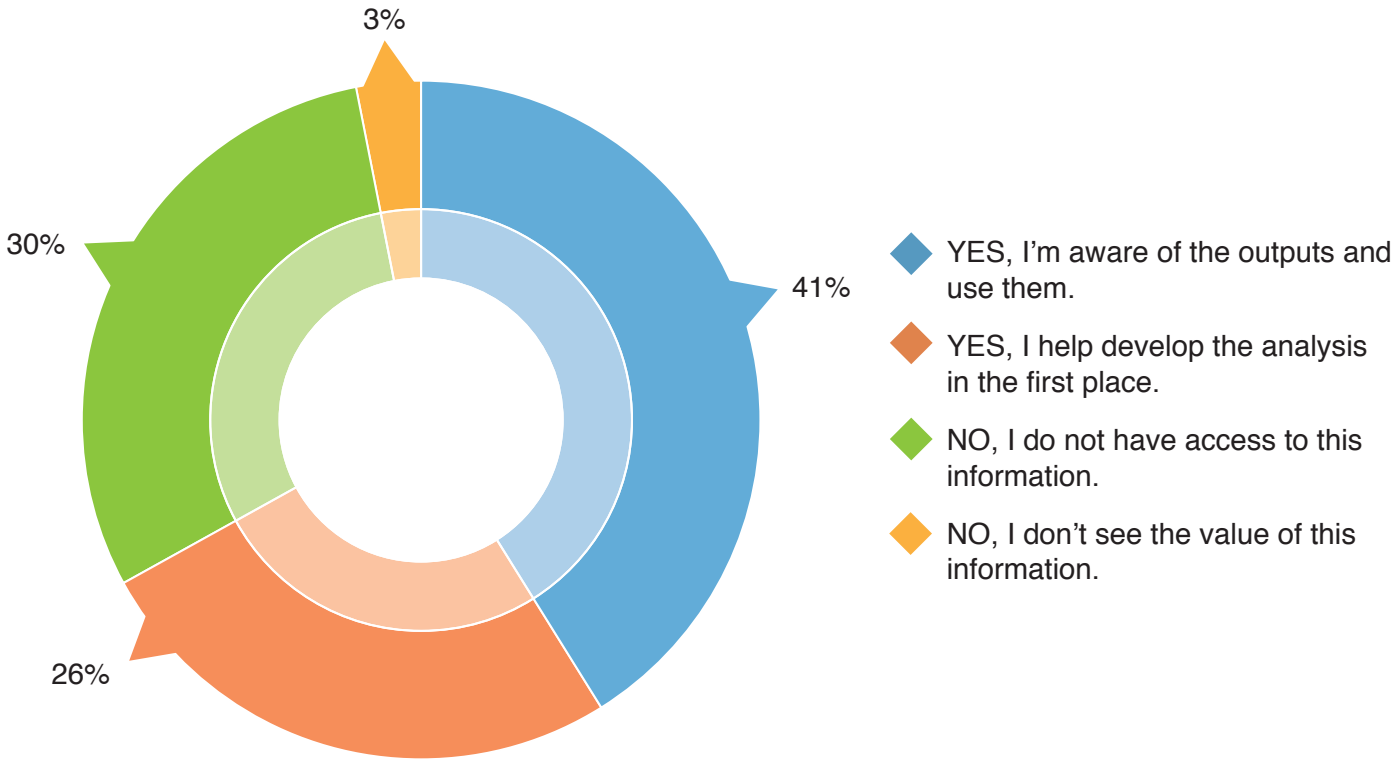


Figure 4. Question 9: As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme? (e.g. to develop scenarios or consider areas of future capability development) (Answers are expressed as percentage, N=492)

The figures show a slight increase in organizations reporting greater BC investment from 23% to 24%. Large businesses are likelier to increase their BC budgets this year than SMEs at 26% compared to 21%. Among industry sectors, manufacturers (42%), retailers (37%) and IT/telecommunications organizations (30%) report greater spending on BC. This improved outlook is especially significant in the case of manufacturing as the percentage of organizations reporting increased budgets have risen from 19% to 42%. A similar observation is made for IT/telecommunications organizations which report bigger BC spends from 12% to 30%. Meanwhile, the worst outlook for BC spending remains in the education, healthcare and public sectors, with 20%, 18% and 14% reporting budget cuts respectively.

Case Study:
Increased BC Investment among SMEs

A report from Carbonite revealed a recent trend of SMEs investing more in BC solutions to protect their online resources. A survey of 700 SMEs worldwide revealed that 81% currently have BC arrangements in place, while 72% are planning to invest more in the next two years. Three in four respondents listed the risk of website downtime as the main threat to profits. It is estimated that an hour of disruption can cost from $8,200 to $25,600, with recovery times lasting up to a day[17].

The report also stated that SMEs seem to move towards cloud based solutions to achieve better BC which offers greater protection against attacks and more solid back-up plans. Indeed, companies are likely to spend as much as 14% of their overall IT annual budget in three or four disaster recovery systems at the same time, reaching an overall investment of about $3,000[18]. Further research from the BCI has also highlighted that SMEs are concerned with the same threats as large enterprises, with the difference that smaller businesses might sometimes have less capacity to implement appropriate counter measures[19]. Nonetheless, a strong BC culture can also make a critical difference in facing security challenges, which means that money spent on training staff can be as vital as that spent on technology.

17. http://www.carbonite.com/en/resources/carbonite-blog/small-businesses-to-invest-more-in-business-continuity-solutions/
18. http://globenewswire.com/news-release/2015/04/28/729165/10130889/en/SMBs-Worldwide-to-Increase-Investments-in-Cloud-and-Hybrid-Business-Continuity-Solutions.html
19. http://www.thebci.org/index.php/about/news-room#/news/small-businesses-investing-more-in-business-continuity-115301

Among regions, organizations based in the Middle East/North Africa and North America strongly outperform the global average (24%) at 37%. Budget cuts are likely to be expected for organizations based in Central and Latin America (33%) however. Figure 5 summarises the overall results.

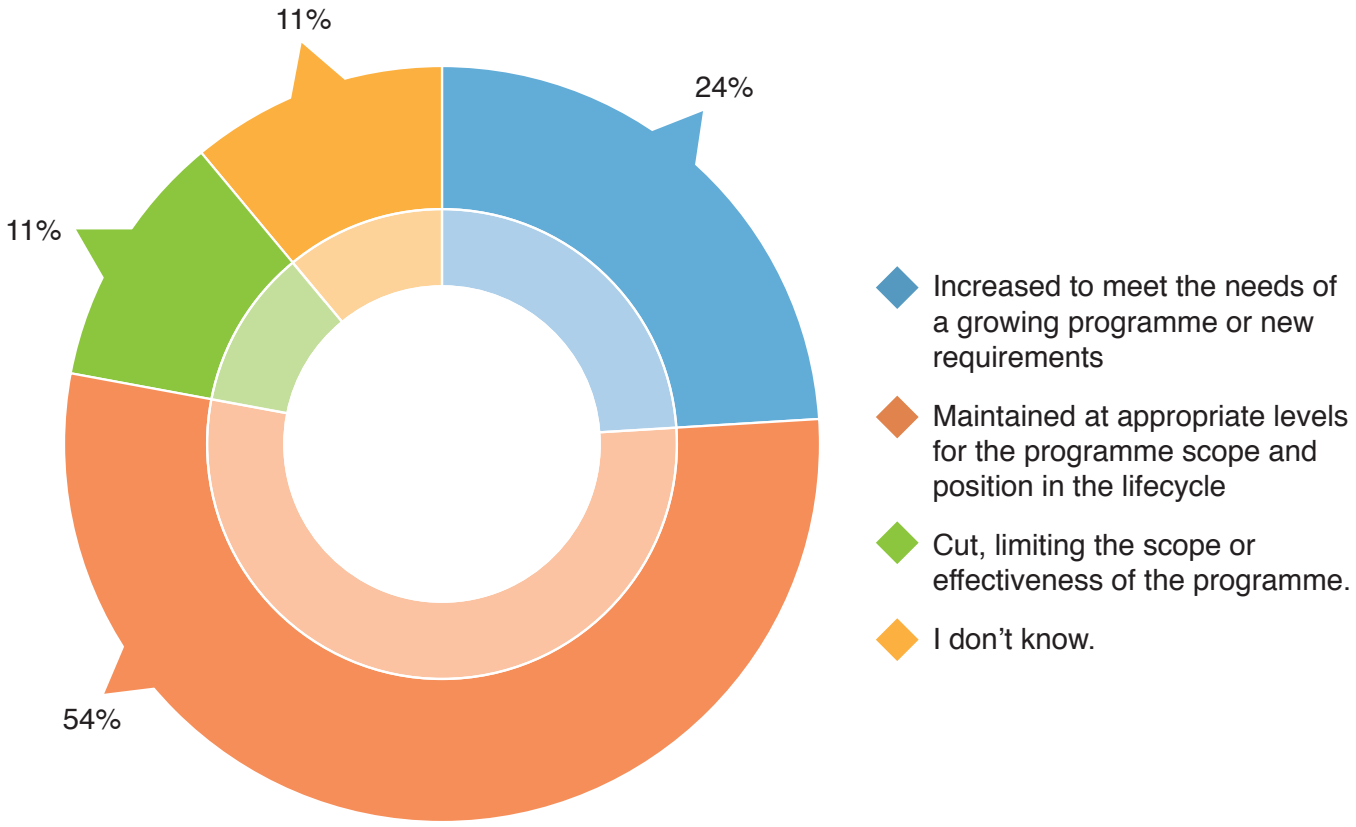


Figure 5. Question 11: If you have an existing business continuity programme, how will investment levels in 2016 compare to the current year? Investment will be... (Numbers are expressed as percentage, N=495)

ISO 22301 Uptake

More than half (51%) of organizations report using ISO 22301 as a framework for the BCM programmes (Figure 6). This uptake of ISO 22301 coincides with earlier BCI research which states that 6 out of 10 organizations adopt the standard in various forms (certification, compliance and alignment)[20].

Comparing SMEs and large businesses reveal an even result at 51%. Looking across industry sectors, the most widespread uptake of ISO 22301 is observed in IT/telecommunications (66%), professional services (56%) and finance (53%). Among regions, organizations based in the Middle East/North Africa (57%), Oceania (53%) and Europe (52%) outstrip the global average. Figure 6 summarises the results.

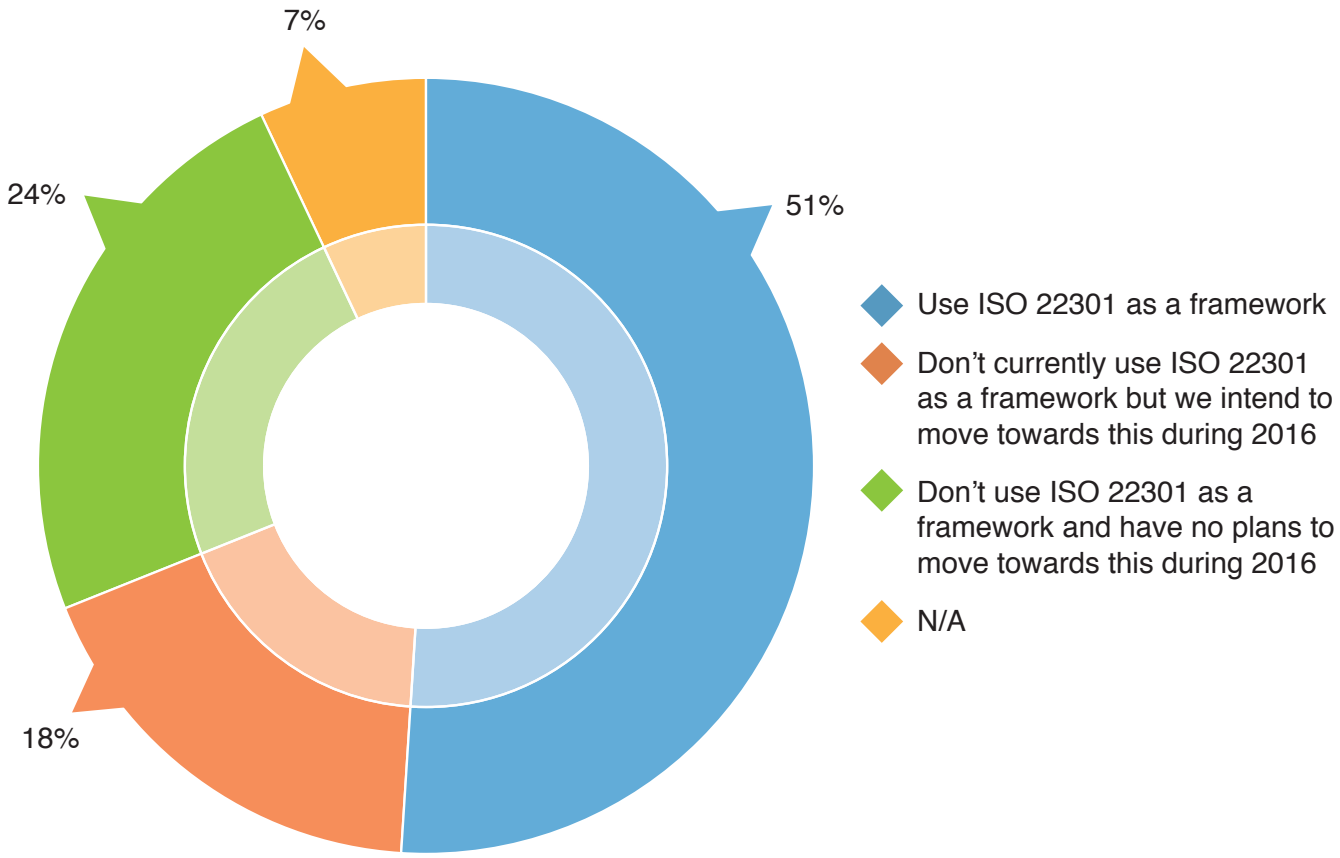


Figure 6. Question 6: If you have a formal business continuity management programme in place, how does it relate to ISO 22301? (Answers are expressed as percentage, N=555)

These results reflect industry trends which show the increasing use of standards in supplier assurance (45% to 49%)[21]. Prior BCI research also reveals that demonstrating assurance of continued service to customers (61%), protecting reputation and brand (48%), reducing business interruption (48%) and building greater resilience against disruption (45%) are the top drivers for standards use[22].

20. Data from the 2015 BCI ISO 22301 Benchmarking Survey
21. Comparison from the 2014 and 2015 BCI Supply Chain Resilience Reports
22. Data from the 2015 BCI ISO 22301 Benchmarking Survey

3 | Conclusion

Conclusion

Horizon scanning impacts on overall resilience as it provides an objective basis for assessing near-term threats that lead to business disruption. Used with longer-term trend analysis, horizon scanning can help organizations build resilient business performance and protect their brand, reputation and bottom line. The BCI Horizon Scan Report, as a global study aggregating practitioner input across industry sectors and regions, complements in-house analysis and provides useful input for strategic decisions. In closing, the following comprise some of the key insights uncovered in this year's research

1 Cyber issues continue to dominate the threat landscape.

Cyber attacks and data breaches consistently figure in horizon scanning results and practitioners are getting increasingly concerned about its potential for damage given the increased sophistication of hostile elements. Related BCI studies demonstrate how these incidents trigger the activation of plans, disrupt supply chains and hurt business reputation.

2 The 'human factor' (i.e. skills shortage, loss of key employees) clearly impacts on business performance and requires a strategic response.

In a rapidly changing, complex business environment, organizations will increasingly rely on retaining key skills and staff as well as relevant succession planning. As the unavailability of talents and key skills make a comeback as one of the top threats in the BCI Horizon Scan Report, this should alert organizations in revisiting their plans for hiring, retention and succession.

3 While many organizations perform trend analysis, its impact on BCM programmes remains limited for some.

A third of organizations do not use trend analysis results at all with access being a key barrier. This is a key weakness which impacts on building resilience across the organization. This strengthens the case for breaking down silos and encouraging engagement especially among protective disciplines such as BC, risk management, information security and others.

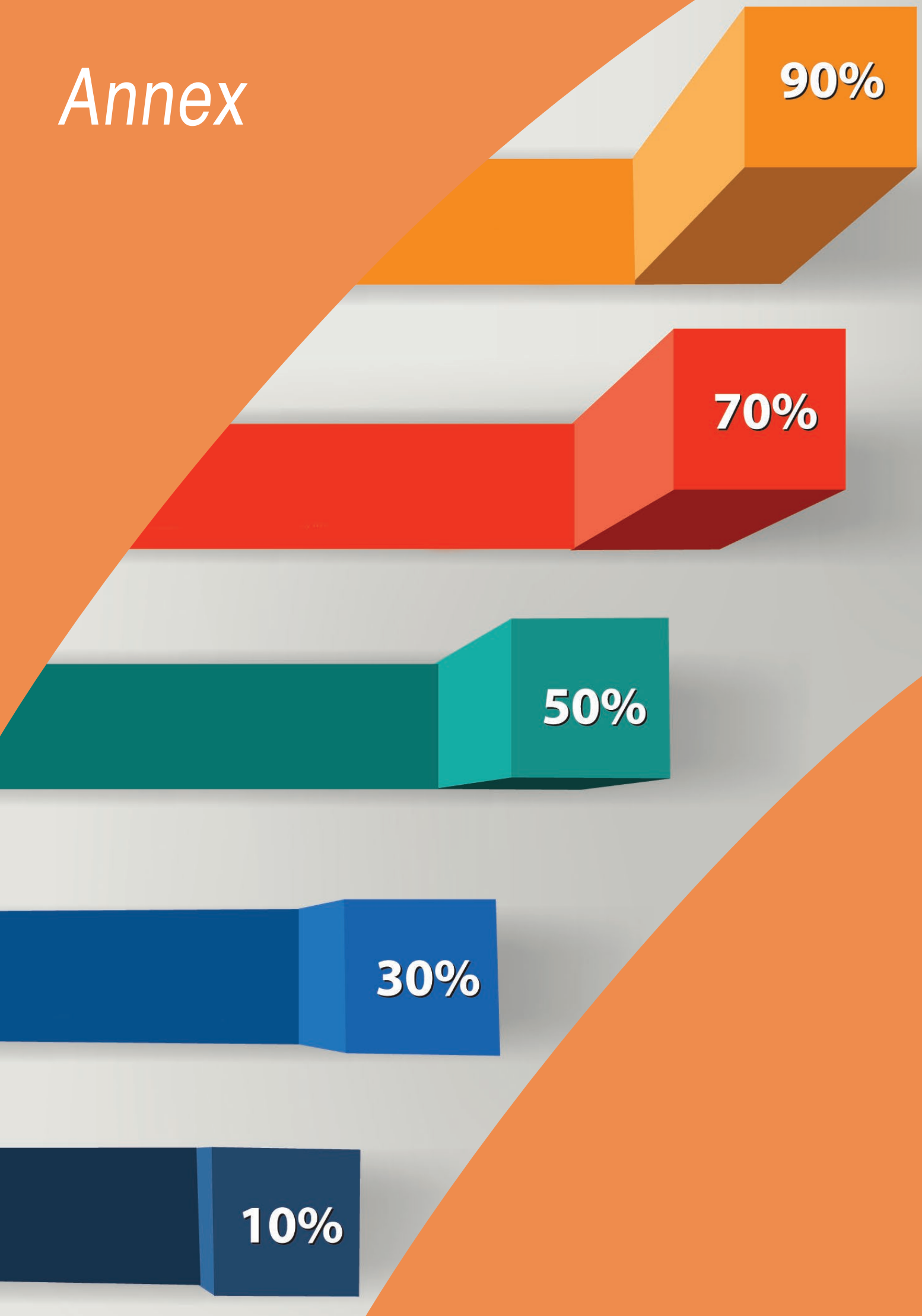
4 There is a generally positive outlook for BC spending but challenges remain in justifying this investment in some industry sectors and regions.

The growth of spending in sectors such as manufacturing, retail and IT/telecommunications may reflect improving economic prospects. However, the squeeze in public spending in many places, reflected especially in the education, public and health care sectors continue to exert pressures on many BC and resilience practitioners.

5 Standards exert increasing influence over BCM programmes and resilience practice.

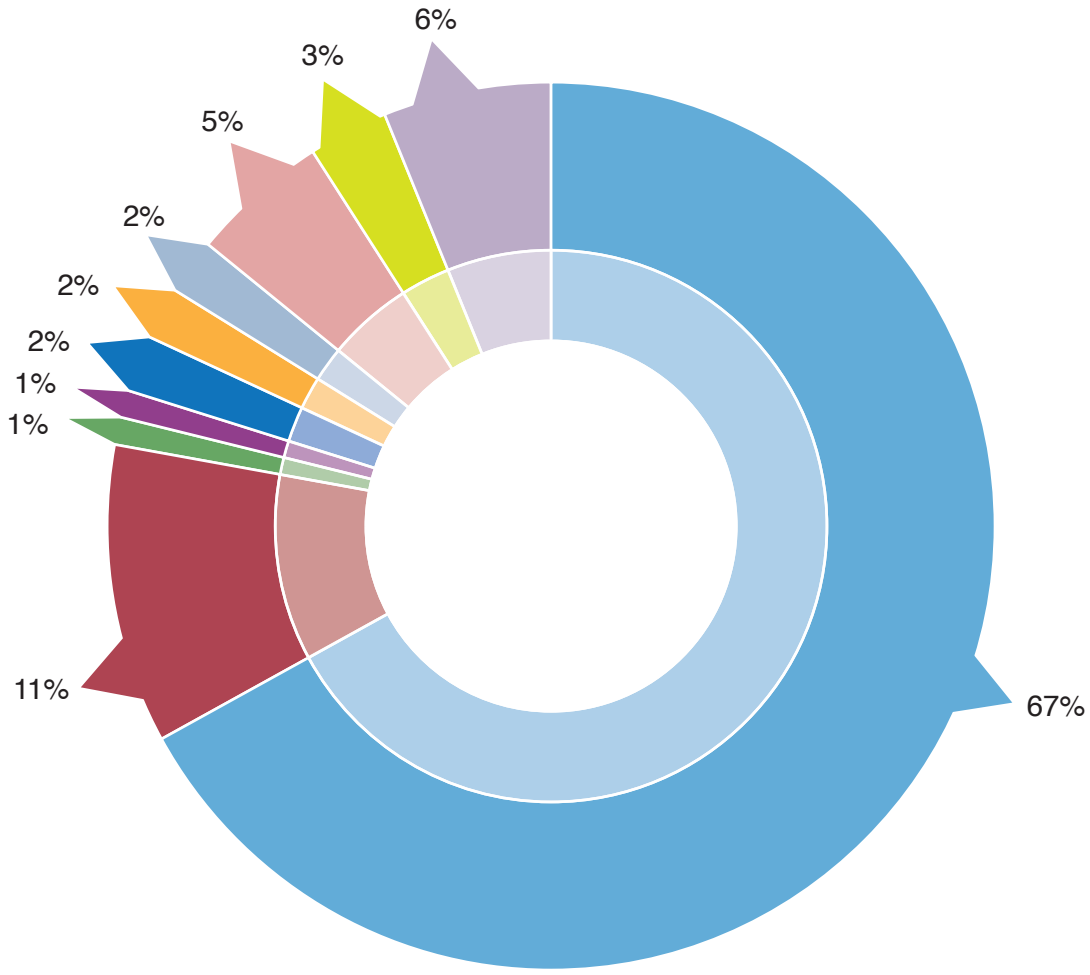
The BCI Horizon Scan Report and related research reveal the broad adoption of standards and its use in providing supplier and customer assurance. Variations remain among industry sectors and it is important to focus future studies on the reasons driving such difference.

Annex



1. Demographic Information

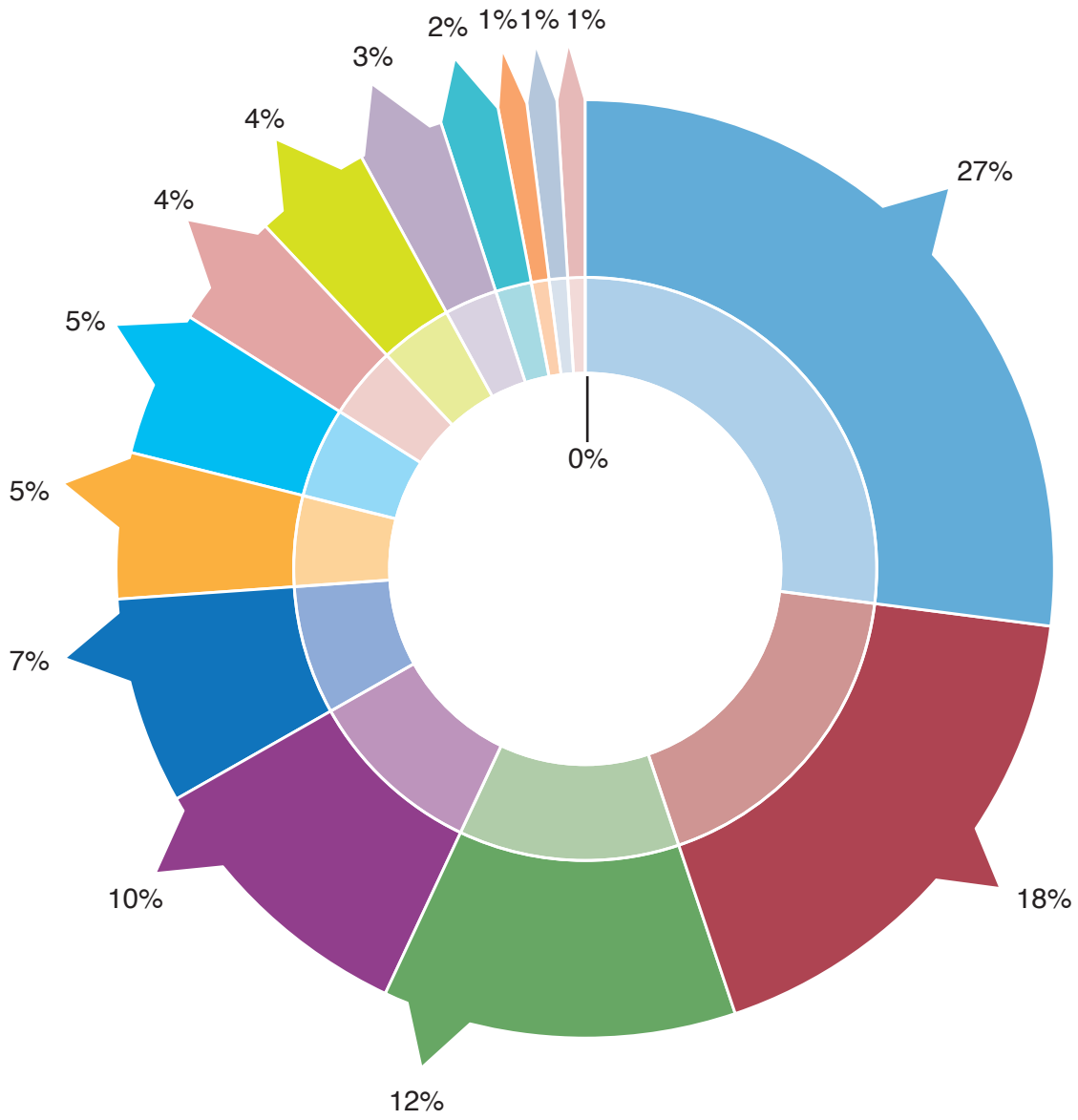
a. Functional Role of the Respondents



- Business Continuity
- Risk Management
- Supply chain/logistics/procurement/purchasing
- Internal Audit
- Line of Business/Service Directorate
- Quality/Business Improvement
- Health & Safety management
- Emergency Planning
- Security (physical/virtual)
- IT Disaster Recovery/IT Service Continuity

Question 1: Which of the following best describes your functional role? (Numbers are expressed as percentage, N=568)

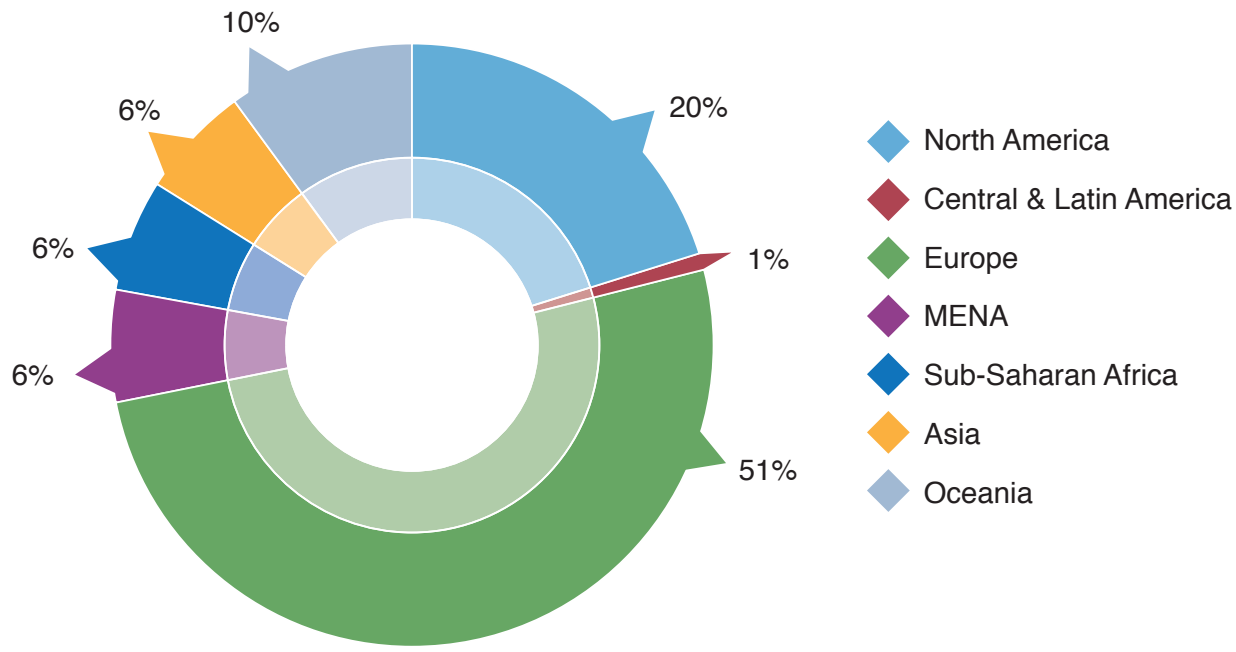
b. Industry Sector



- Financial & Insurance Services
- Professional Services
- IT & Communications
- Public Administration & Defence
- Health & Social Care
- Manufacturing
- Energy & Utility Services
- Education
- Retail & Wholesale
- Transport & Storage
- Media & Entertainment
- Engineering & Construction
- Support Services
- Agriculture, Forestry & Fishing
- Mining & Quarrying

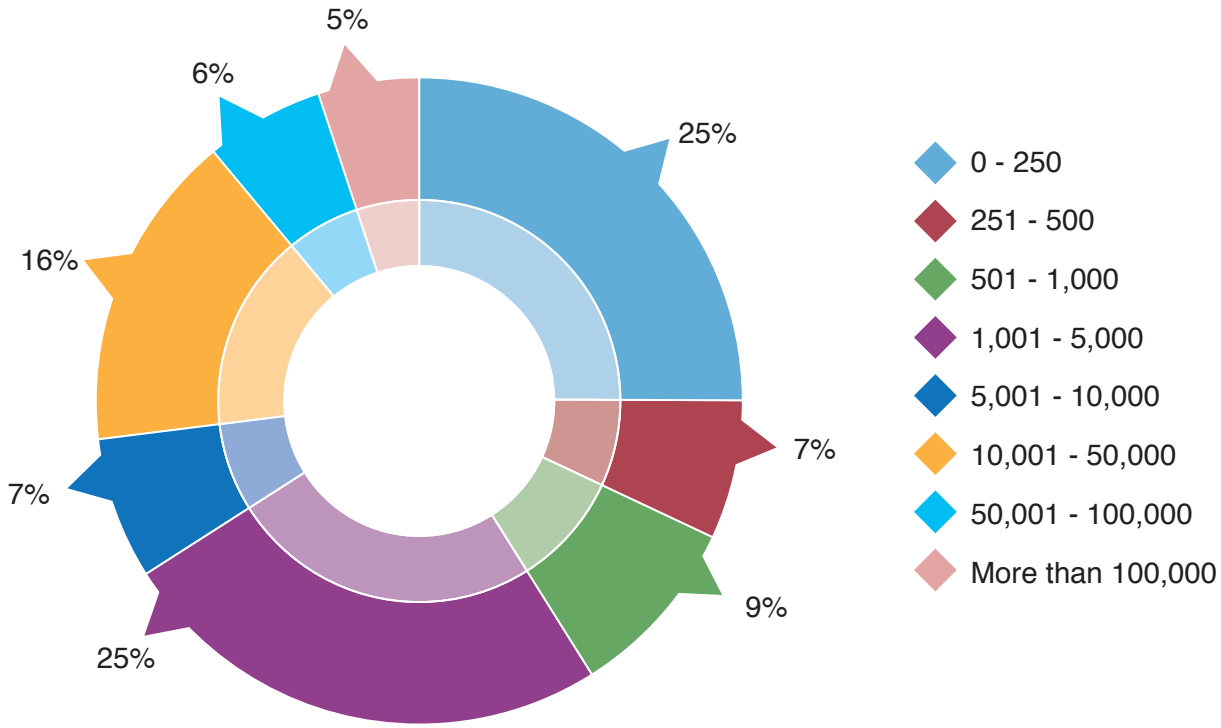
Question 2: Please indicate the primary activity of your organization using the SIC 2007 categories given below (Numbers are expressed as percentage, N=568)

c. Geographical Base



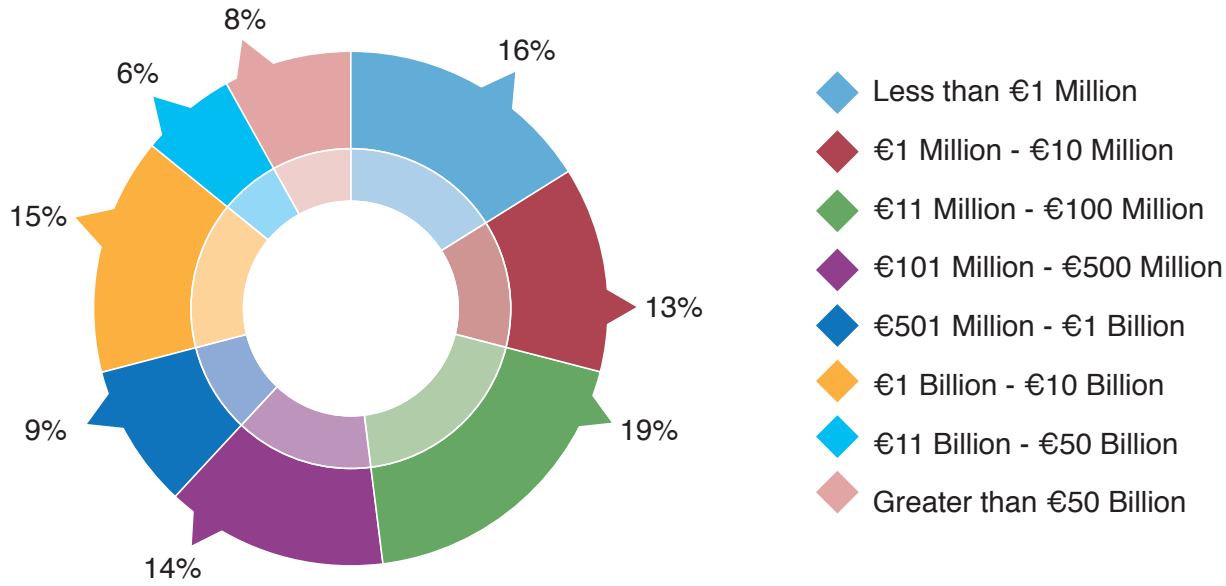
Question 3: Which country are you based in? (Numbers are expressed as percentage, N=568)

d. Number of Employees



Question 4: How many employees are there in your organization? (Numbers expressed as percentage, N= 568)

e. Approximate Annual Revenues



Question 5: What is your organization's annual turnover? (Numbers are expressed as percentage, N=568)

2. COMPARISON BY REGION/COUNTRY

	Europe	North America	Asia	Oceania
Top three threats (Based on extremely concerned responses)	Cyber attack-50%	Cyber attack-49%	Cyber attack-42%	Cyber attack-44%
	Data breach-42%	Data breach-46%	Unplanned IT and Telecom outages-39%	Data breach-40%
	Unplanned IT & telecom outages-34%	Unplanned IT & telecom outages-32%	Data breach-35%	Unplanned IT & telecom outages-36%
Top three trends	Use of Internet for malicious attacks-85%	Use of internet for malicious attacks-85%	Use of Internet for malicious attacks-79%	Use of internet for malicious attacks-85%
	Influence of social media-64%	Influence of social media 67%	Potential emergence of a global pandemic-57%	Influence of social media-64%
	Loss of key employee-58%	New regulations & increased regulatory scrutiny-61%	Influence of social media-54%	Prevalence and high adoption of internet dependent services-60%
Conducting Trend Analysis	72%	70%	75%	75%
Use of ISO 22301	52%	50%	50%	53%
Level of BC Investment	Up- 20% Down- 13% Unchanged-57%	Up-37% Down-6% Unchanged-50%	Up-26% Down-15% Unchanged-48%	Up -16% Down -13% Unchanged-60%

2. COMPARISON BY REGION/COUNTRY

	Middle East & North Africa	Central and Latin America	Sub-Saharan Africa	UK
Top three threats (Based on extremely concerned responses)	Cyber attack-50%	Adverse weather-43%	Interruption to utility supply-60%	Cyber attack-49%
	Unplanned IT & telecom outages-47%	Business ethics-43%	Cyber attack-40%	Data breach-39%
	Data breach-44%	Environmental incident-43%	Exchange rate volatility-40%	Unplanned IT & telecom outages-33%
Top three trends	Loss of key employee-73%	Political change 86%	Use of internet for malicious attacks-77%	Use of internet for malicious attacks-85%
	Political change-63%	Use of internet for malicious attacks-86%	Political change-70%	Influence of social media-67%
	Use of internet for malicious attacks-63%	Climate change 71%	Energy security & the transition to sustainable energy infrastracutres-60%	Loss of key employee-61%
Conducting Trend Analysis	57%	29%	70%	72%
Use of ISO 22301	57%	50%	41%	53%
Level of BC Investment	Up-37% Down-3% Unchanged -37%	Up-17% Down-33% Unchanged-33%	Up-20% Down-10% Unchanged-50%	Up-19% Down-12% Unchanged-61%

	US	Australia	Canada	Netherlands
Top three threats (Based on extremely concerned responses)	Cyber attack-51%	Cyber attack-43%	Cyber attack-29%	Cyber attack-57%
	Data breach-51%	Data breach-43%	Data breach-24%	Data breach-50%
	Unplanned IT & telecom outages-34%	Unplanned IT & telecom outages-35%	Adverse weather-18%	Unplanned IT & telecom outages-43%
Top three trends	Use of internet for malicious attacks-88%	Use of Internet for malicious attacks 84%	Influence of social media-76%	Use of internet for malicious attacks-86%
	Influence of social media-64%	Influence of social media-73%	Use of internet for malicious attacks-76%	Increasing supply chain complexity-64%
	New regulations & increased regulatory scrutiny-62%	Prevalence and high adoption of Internet dependent services-54%	Loss of key employee-53%	Influence of social media-64%
Conducting Trend Analysis	70%	78%	94%	86%
Use of ISO 22301	51%	56%	44%	44%
Level of BC Investment	Up-35% Down-5% Unchanged -53%	Up-14% Down-14% Unchanged-65%	Up-29% Down-12% Unchanged-47%	Up-21% Down-7% Unchanged-50%

3. COMPARISON BY INDUSTRY SECTOR

	Financial & Insurance	Professional Services	Manufacturing	Public Admin & Defence
Top three threats (Based on extremely concerned responses P4	Cyber attack-56%	Cyber attack-47%	Supply chain disruption-46%	Cyber attack-48%
	Data breach-46%	Data breach-41%	Cyber attack-27%	Data breach-46%
	Unplanned IT & telecom outages-34%	Unplanned IT & telecom outages-34%	Data breach-27%	Unplanned IT & telecom outages-36%
Top three trends P5	Use of internet for malicious attacks-91%	Use of internet for malicious attacks-82%	Increasing supply chain complexity-73%	Use of internet for malicious attacks-84%
	Influence of social media 67%	Influence of social media 67%	Use of internet for malicious attacks-62%	Potential emergence of a global pandemic-65%
	New regulations and increased regulatory scrutiny-64%	Loss of key employee-62%	Loss of key employee-58%	Influence of social media 61%
Conducting Trend Analysis P5	76%	62%	62%	86%
Use of ISO 22301 P3	53%	56%	48%	47%
Level of BC Investment P6	Up-26% Down-6% Unchanged -61%	Up-21% Down-9% Unchanged-57%	Up-42% Down-15% Unchanged-19%	Up-14% Down-14% Unchanged-61%

	IT & Communications	Health & Social Care	Retail & Wholesale	Education
Top three threats (Based on extremely concerned responses P4	Cyber attack-59%	Unplanned It & telecom outages-41%	Data breach-60%	Unplanned IT & telecom outages-43%
	Data breach-50%	Data breach-41%	Cyber attack-50%	Interruption to utility supply-29%
	Unplanned IT & telecom outages-47%	Cyber attack-38%	Unplanned IT & telecom outage-40%	Act of terrorism-29%
Top three trends P5	Use of internet for malicious attacks-86%	Potential emergence of a global pandemic-74%	Use of internet for malicious attacks-79%	Use of internet for malicious attacks-95%
	Loss of key employee-56%	Use of internet for malicious attacks-71%	Influence of social media-63%	Influence of social media-85%
	New regulations and increased regulatory scrutiny-56%	Influence of social media-68%	Increasing supply chain complexity-63%	Political change-75%
Conducting Trend Analysis P5	64%	53%	48%	65%
Use of ISO 22301 P3	66%	50%	29%	18%
Level of BC Investment P6	Up-30% Down-7% Unchanged -53%	Up-24% Down-18% Unchanged-41%	Up-37% Down-21% Unchanged-42%	Up-15% Down-20% Unchanged-50%

4. COMPARISON BY BUSINESS SIZE

	SMEs	Large businesses
Top three threats (Based on extremely concerned responses)	Cyber attack-39%	Cyber attack-51%
	Data breach-33%	Data breach-44%
	Unplanned IT & telecom outages-30%	Unplanned IT & telecom outages-37%
Top three trends	Use of internet for malicious attacks-81%	Use of internet for malicious attacks-84%
	Influence of social media-66%	Influence of social media-62%
	Loss of key employee-65%	New regulations & increased regulatory scrutiny-54%
Conducting Trend Analysis	58%	74%
Use of ISO 22301	51%	51%
Level of BC Investment	Up-21% Down-12% Unchanged -58%	Up-26% Down-11% Unchanged-52%

About the Authors

Patrick Alcantara DBCI (BCI Senior Research Associate) wrote this report. He is a senior research practitioner with extensive publication, project management and public speaking experience. He has delivered research projects for organizations such as Zurich, BSI and the UK Department of Business Innovation & Skills. He is also part of the Editorial Board of the international, peer-reviewed Journal of Business Continuity & Emergency Planning. He obtained a Diploma in Business Continuity Management from Bucks New University and was awarded a Distinction for a Masters by the Institute of Education (now University College London) and Deusto University. He can be contacted at patrick.alcantara@thebci.org.

Gianluca Riglietti wrote the Annex and case studies. He has also performed additional research for this report. He is a Research Assistant for the BCI. He recently finished his MA in Geopolitics, Territory and Security from King's College London. His previous professional experience includes working for the Italian presidency of the Council of Ministers in the European Union. He can be contacted at gianluca.riglietti@thebci.org.

Acknowledgements

We would like to thank BSI for supporting this research for the fifth year running.

We also acknowledge Carla Whyte (BSI UK Client Propositions Manager) for her assistance during the survey period. Andrew Scott CBCI (BCI Senior Communications Manager) reviewed this report.

About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the Business Continuity Institute (BCI) has established itself as the world's leading Institute for business continuity and resilience. The BCI has become the membership and certifying organization of choice for business continuity and resilience professionals globally with over 8,000 members in more than 100 countries, working in an estimated 3,000 organizations in the private, public and third sectors.

The vast experience of the Institute's broad membership and partner network is built into its world class education, continuing professional development and networking activities. Every year, more than 1,500 people choose BCI training, with options ranging from short awareness raising tools to a full academic qualification, available online and in a classroom. The Institute stands for excellence in the resilience profession and its globally recognised Certified grades provide assurance of technical and professional competency. The BCI offers a wide range of resources for professionals seeking to raise their organization's level of resilience, and its extensive thought leadership and research programme helps drive the industry forward. With approximately 120 Partners worldwide, the BCI Partnership offers organizations the opportunity to work with the BCI in promoting best practice in business continuity and resilience.

The BCI welcomes everyone with an interest in building resilient organizations from newcomers, experienced professionals and organizations. Further information about the BCI is available at www.thebci.org.

Business Continuity Institute

Contact the BCI

Andrew Scott
Senior Communications Manager

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

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

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, Automotive, Built Environment, Food, Healthcare and ICT. With 80,000 clients in 182 countries, BSI is an organization whose standards inspire excellence across the globe.

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

Contact the BSI

Carla Whyte
Client Propositions Manager

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

+44 (0)345 080 9000
carla.whyte@bsigroup.com

Business Continuity Institute

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

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

Correct as of January 2016