Business Continuity Institute

HORIZON SCAN REPORT 2017

Business Continuity Institute

bsi.

Foreword
Business Continuity Institute (BCI)

David Thorp
BCI Executive Director

I'm delighted to introduce the Business Continuity Institute Horizon Scan Survey 2017. This is one of our most popular and influential pieces of research and is now being published for the sixth consecutive year with the support of BSI. These are uncertain times with multiple challenges in the macro and micro environments in which we all operate and it has never been more important for an organization to take an objective view of the challenges that are out there.

Horizon scanning techniques are one of the most critical tools at the disposal of BC and resilience professionals. Used effectively they can deliver clear insights into fast-changing threat landscapes. Knowing what your organization is up against will help it become resilient and ride out the challenging conditions we currently seem to be looking at in order not only to survive in the immediate future but to go on to thrive long term.

Given the diversity of the threats out there, it is absolutely essential to adopt agile and dynamic responses. Planning to recover from a data breach is very different from planning for the aftermath of a terrorist attack, and, as this year's report highlights, the risk spectrum can be very broad. Malicious internet actors, political shake-ups, and climate change are all amongst the main worries for societies around the world.

Cyber-attacks and data breaches continue to cost organizations billions of dollars annually, a sum that is only likely to go up with the increasing integration of new pieces of technology into daily operations and the consequent reliance on connectivity. Cutting-edge devices, such as those belonging to the so-called "Internet of Things", are offering great opportunities for organizations but this can come at the cost of increased vulnerability to hostile actors. It is essential therefore to be aware of these vulnerabilities and to devise suitable plans and responses to the threats to continuity they represent. Only by doing so can your organization be considered resilient.

Politics too has been a dominant topic this year, certainly more than in the recent past. Unexpected political outcomes have shaken some of the previous "certainties" in Western countries. From Brexit to the US elections the changes such decisions herald might be significant and far-reaching, and in this global society we now enjoy this goes way beyond the national borders of those directly affected and opens all of us up, wherever we might be, to a wave of change that will probably impact long-standing trade agreements and economic stability. Whether this is for better or worse, only time will tell, but the uncertainty created in the past twelve months is likely to cascade down on organizations in the near to medium future.

Extreme weather events too have been a great cause of disruption in recent years, becoming less and less predictable with the apparent acceleration of climate change. While the recent Paris agreement could be a step forward in the longer term, at present adverse weather impacts are a fact of life and represent considerable risk for many organizations and appropriate responses need to be developed by organization thus affected.

As always, the key takeaway should be that with challenges come opportunities. Change does not have to mean less favourable environments, but the landscape may be different. As organizations venture into uncharted territory now is the time to identify and undertake the measures that will increase resilience within your organization by ensuring that effective business continuity planning is in place.

Foreword
BSI

Howard Kerr

BSI Chief Executive

The release of the 2017 BCI Horizon Scan Report marks the sixth year of the Horizon Scan publishing partnership between BSI and the BCI. In the time our two organizations have worked together the environment in which businesses operate has changed significantly. Greater challenges have surfaced from increasingly sophisticated cybercrime, terror attacks, political shifts, economic instability and climate change. As these threats grow in number and significance, so too does the value of business continuity.

This year, the top three perceived threats—cyber attacks, data breaches and unplanned IT and telecom outages—are directly related to technology and the ability to protect, manage and access information. These threats are very real and, unsurprisingly, are related to three of the top four disruptions that were actually experienced: unplanned IT and telecom outages (1), cyber attacks (3) and security incidents (4). How organizations protect, access and dispose of their information-based assets throughout their lifecycle is directly related to the depth of their information resilience or ability to safeguard sensitive information. Organizations that do not take these threats seriously and develop plans to manage them, are exposing themselves to both financial and reputational loss, if not ruin.

Data protection is a growing concern for businesses. According to the Information Security Breaches Survey 2015, carried out for the UK government's business department by PwC, there has been an increase in the number of both large and small organizations experiencing IS breaches, with a staggering 90% of large organizations and 74% of small firms suffering a breach in the last 12 months. These findings clearly suggest that being subject to a breach is no longer an 'if' proposition but 'when'. Organizations that have embedded business continuity are better prepared for the latter.

On the bright side, this report indicates that businesses are looking to bolster their ability to not just survive but thrive in times of adversity. More than 2 out of 3 organizations (69%) are conducting longer term trend analysis as part of their horizon scanning activity and 63% are grounding their business continuity in best practice by using ISO 22301 as a guide. Anticipating the worst and planning how to manage it is the backbone of business continuity. It requires both time and resources that may be difficult to justify in the moment, but much like the value of paying fire insurance premiums, its value is very much appreciated after a fire.

However, organizations must also recognize that where there is risk, there is also opportunity. Therefore organizations should also focus on business improvement. Organizational Resilience reaches beyond risk management towards a more holistic view of business health and success. And, in today's dynamic interconnected world, the ability of an organization to anticipate, prepare for, respond to and adapt to change - and crucially to prosper from it - is more important than ever.

Contents

Section 1

Executive Summary 1

Section 2

Horizon Scan Report 2017 4

Section 3

Conclusion 18

Section 4

Annex 20

1 Executive Summary

BCI Horizon Scan 2017

726 responding organizations

79 countries

Top 10 threats

- 1st Cyber attack
- 2nd Data breach
- 3rd Unplanned IT and telecom outages
- 4th Security incident
- 5th Adverse weather
- 6th Interruption to utility supply
- 7th Act of terrorism
- 8th Supply chain disruption
- 9th Availability of talents/key skills
- 10th New laws or regulations

Top 10 disruptions

- 1st Unplanned IT and telecom outages
- 2nd Adverse weather
- 3rd Interruption to utility supply
- 4th Cyber attack
- 5th Security incident
- 6th Transport network disruption
- 7th Availability of talents/key skills
- 8th Supply chain disruption
- 9th Data breach
- 10th New laws or regulations

Top 10 trends

1st Use of internet for malicious attacks

2nd Influence of social media

3rd Loss of key employee

4th New regulations and increased regulatory scrutiny

5th Prevalence and high adoption of internet dependent services

6th Political change

7th Increasing supply chain complexity

8th Potential emergence of a global pandemic

9th Changing consumer attitudes and behaviour

10th Slow economic growth and its impact on investment

Trend analysis

(69%)
More than 2 out of 3 organizations conduct longer term trend analysis as part of their horizon scanning activity

Investment in business continuity capability

(21%)
1 out of 5 organizations will increase their budgets for business continuity in 2017

ISO 22301 uptake

(63%)
More than 2 out of 3 organizations use ISO 22301 in guiding their business continuity programme

2 | Horizon Scan Report 2017

In association with BSI, the BCI Horizon Scan Report is based on an annual study which tracks near-term threats to organizations across industry sectors globally. In its sixth edition, this study measures concern over specific threats as reported by business continuity and resilience professionals. The report also captures disruption caused by these threats, offering a basis of comparison between the level of concern and actual incidents.

Over the years, this report has become a highly anticipated industry resource as it complements in-house analysis and assists horizon scanning activity. The report features results of a survey which was distributed from October 2016 and ran for four weeks; 726 organizations from 79 countries participated in this study.

Case Study:
Climate change increases business risks

Research confirms that climate change is already increasing risks for businesses in the United Kingdom (UK). The shift in average temperatures due to greenhouse gases is likely to bring more weather related hazards and cause disruptions to organizations. Other research confirms that climate change is referred to as a 'risk multiplier'[1], since it interacts with other types of threats and increases vulnerabilities.

Flooding, already considered a significant problem in the UK, is bound to become more severe and frequent due to a changing climate, affecting businesses and communities. Infrastructure might be at risk too, hindering operations and affecting revenues. Natural disasters might also reduce productivity, resulting in price swings that would bring uncertainty to both domestic and foreign economies. In addition, more humid conditions have the potential to favour the spread of new diseases that could harm both people and wildlife[2]. For example, the UK transport network was recently disrupted by more extreme weather conditions. Heavier than usual rain caused reduced service and overcrowded stations[3]; on the other hand, unusually high temperatures in the summer caused severe delays and speed restrictions[4].

Extreme weather events caused by climate change may also have effects on organizations' supply chains. Supply chain disruptions linked to extreme weather events could become expensive, especially when outsourcing goods and services from different countries[5]. In 2010 for instance, Russia was hit by unusually warm temperatures, leading to decreased wheat production. This led to an estimated $15 billion loss, which impacted global supplies of wheat as a consequence of Russia's limited exporting capacity[6].

[1] http://www.pwc.com/gx/en/services/advisory/consulting/risk/resilience/publications/business-not-as-usual.html
[2] https://www.theccc.org.uk/wp-content/uploads/2016/07/UK-CCRA-2017-Synthesis-Report-Committee-on-Climate-Change.pdf
[3] http://www.bbc.co.uk/news/uk-36603508
[4] http://www.bbc.co.uk/news/uk-36833042
[5] http://www.lse.ac.uk/GranthamInstitute/news/british-businesses-at-risk-of-damages-and-disruptions-from-climate-change/
[6] http://www.pwc.com/gx/en/services/advisory/consulting/risk/resilience/publications/business-not-as-usual.html

Measuring concern over specific threats

One of the key metrics the BCI Horizon Scan Report measures is the level of concern by business continuity and resilience professionals over specific threats. The report reveals that the top three threats remain unchanged with cyber attacks retaining first place for the third straight year. Eighty-eight percent (88%) of respondents report being 'extremely concerned' or 'concerned' about this threat materialising. The recent BCI Cyber Resilience Report elaborates on the types of cyber attacks that organizations may face which may include phishing, malware and denial of service[7].

Data breach retains second place in the list of threats with 81% of respondents expressing relatively higher levels of concern[8]. Under half of respondents (47%) notably report that they are 'extremely concerned' over this threat. Unplanned IT and telecommunications outages (80%) remains in third place among threats practitioners are most concerned about.

Security incidents rise from fifth (55% in 2016) to fourth (57% in 2017). Concerns over physical security threats seem to loom larger in the minds of business continuity and resilience professionals. For instance, the most recent BCI Emergency Communications Report noted that around 6 out of 10 organizations (62%) are less confident in their capabilities to respond to location-specific incidents involving physical security (e.g. workplace violence, etc.)[9]. However, concerns over acts of terrorism seem to recede as it falls three places from fourth to seventh at 51% this year.

Respondents show growing concerns over adverse weather as it rises three places from eight to fifth. Rounding out the top 10 are interruption to utility supply (sixth), acts of terrorism (seventh), supply chain disruption (eighth), availability of key talents and skills (ninth) and new laws and regulations (tenth).

Supply chain disruption remains in the top 10 for the third year running. This is an ongoing concern among organizations as more than a third (34%) report losing at least €1 million cumulatively on annual basis due to supply chain losses. 9% report at least €1 million of losses due to a single incident[10].

New laws and regulations enter the top 10 this year. This could be due to concern over changes in legislation that might be brought about by political change such as the recent vote in the UK to leave the European Union. Meanwhile, health and safety incident drops out of the top 10.

Outside of the top 10, concerns over exchange rate volatility rise as it jumps six places from 20th to 14th. Practitioners also seem to be more concerned about business ethics incidents and their impact on brand or company reputation as it rises seven places from 22nd to 15th. Meanwhile, concerns over human illness drops three places from 13th to 16th. Energy cost and availability also drops by four places from 15th to 19th. A full list of threats is shown in Figure 1. Segmented data according to specific regions, countries and industry sectors are available in the Annex of this report.

[7] A copy of the BCI Cyber Resilience Report may be found here: http://www.thebci.org/index.php/obtain-the-cyber-resilience-report-2016.

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

[9] A copy of the BCI Emergency Communications Report may be found here: http://www.thebci.org/index.php/emergency-communications-report-2016

[10] A copy of the BCI Supply Chain Resilience Report may be found here: http://www.thebci.org/index.php/bci-supply-chain-resilience-report-2016

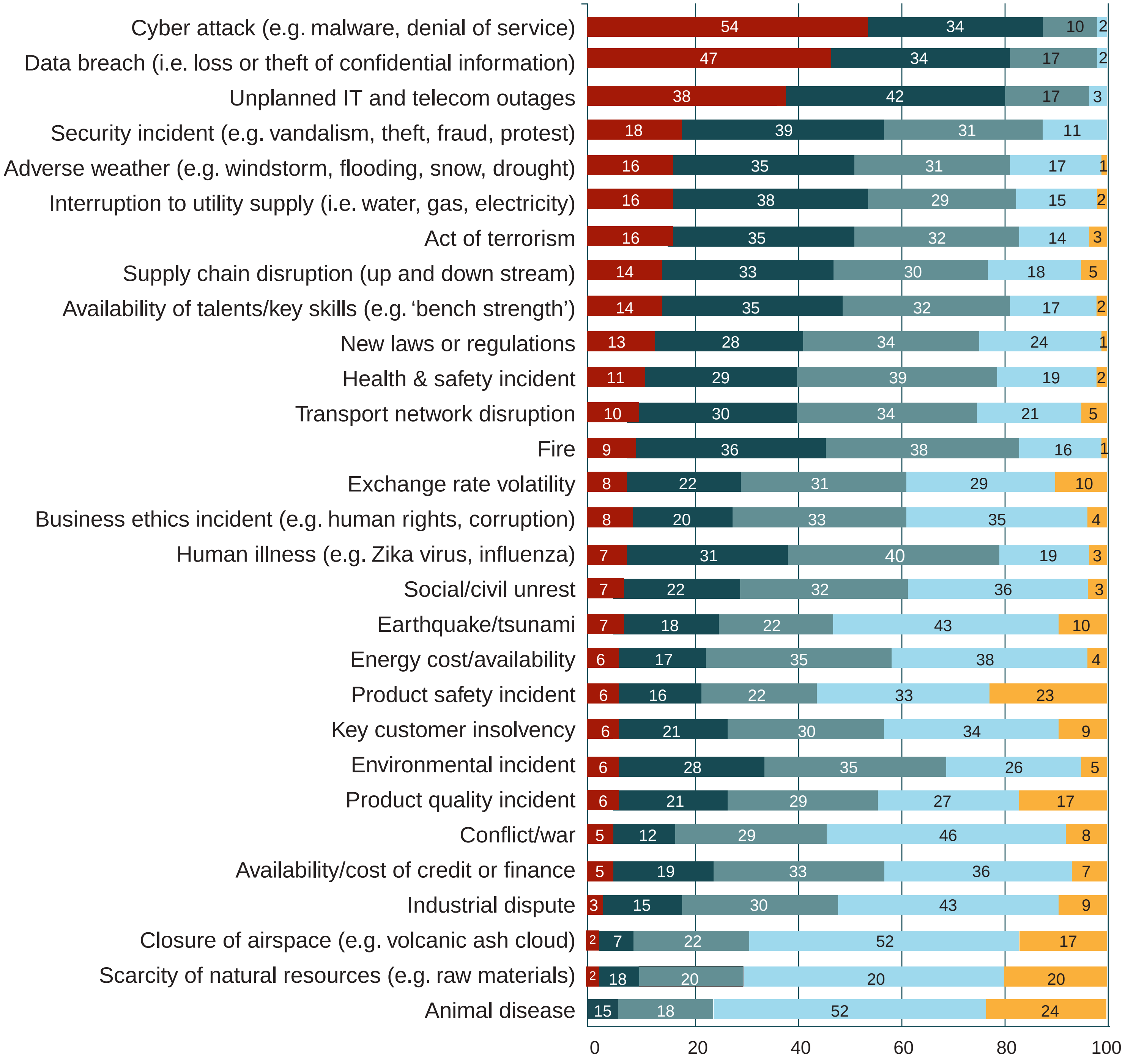


Figure 1. Based on your analysis, how concerned are you about the following threats to your organization in 2017? (N=666, answers expressed in percentage. Multiple responses allowed.)

- ◆ Extremely concerned
- ◆ Concerned
- ◆ Somewhat concerned
- ◆ Not concerned
- ◆ Not applicable

Measuring actual disruption levels

A new metric introduced in the BCI Horizon Scan Report measures actual disruption levels caused by the threats listed in figure 1 in order to provide a comparison against organizations' concerns. Figure 2 shows a contrast between the levels of disruption caused by a particular threat and how concerned an organization is about it.

The study shows the actual causes of business disruption slightly differ from the threats practitioners list as significant concerns. The top causes of business disruption according to the same respondents include unplanned IT and telecommunications outages (72%), adverse weather (43%), interruption to utility supply (40%), cyber attacks (35%) and security incidents (24%). It may be noted that four causes of disruption also figure in the top five during the horizon scanning exercise.

Rounding out the top 10 are transport network disruption (sixth at 19%), availability of key talents and skills (seventh at 18%), supply chain disruption (eighth at 17%), data breach (ninth at 15%) and new laws and regulations (tenth at 14%). Except for transport network disruption which ranked 12th in the Horizon Scan, all causes of disruption are in the top 10 list of threats.

It is interesting to note that while disruption levels roughly coincide with practitioner concern over a specific threat, there are some threats which figure far more to organizations. For example, while more than half of practitioners (54%) are 'extremely concerned' over cyber attacks, over a third of organizations (35%) actually report disruption. Similarly, under half (47%) of practitioners report being 'extremely concerned' about data breaches while 15% of organizations report disruptions caused by it. 16% of practitioners report significant concern over acts of terrorism while only 10% report actual disruptions caused by terrorist activity.

This result underscores that levels of concern over a specific threat may not necessarily coincide with actual disruption. Often, intense media coverage over a specific threat (e.g. cyber attacks, terrorism, etc.) influences organizations' concerns. This finding should encourage organizations to reflect on their concerns and see whether it is proportional to the actual levels of disruption caused by a particular threat materialising.

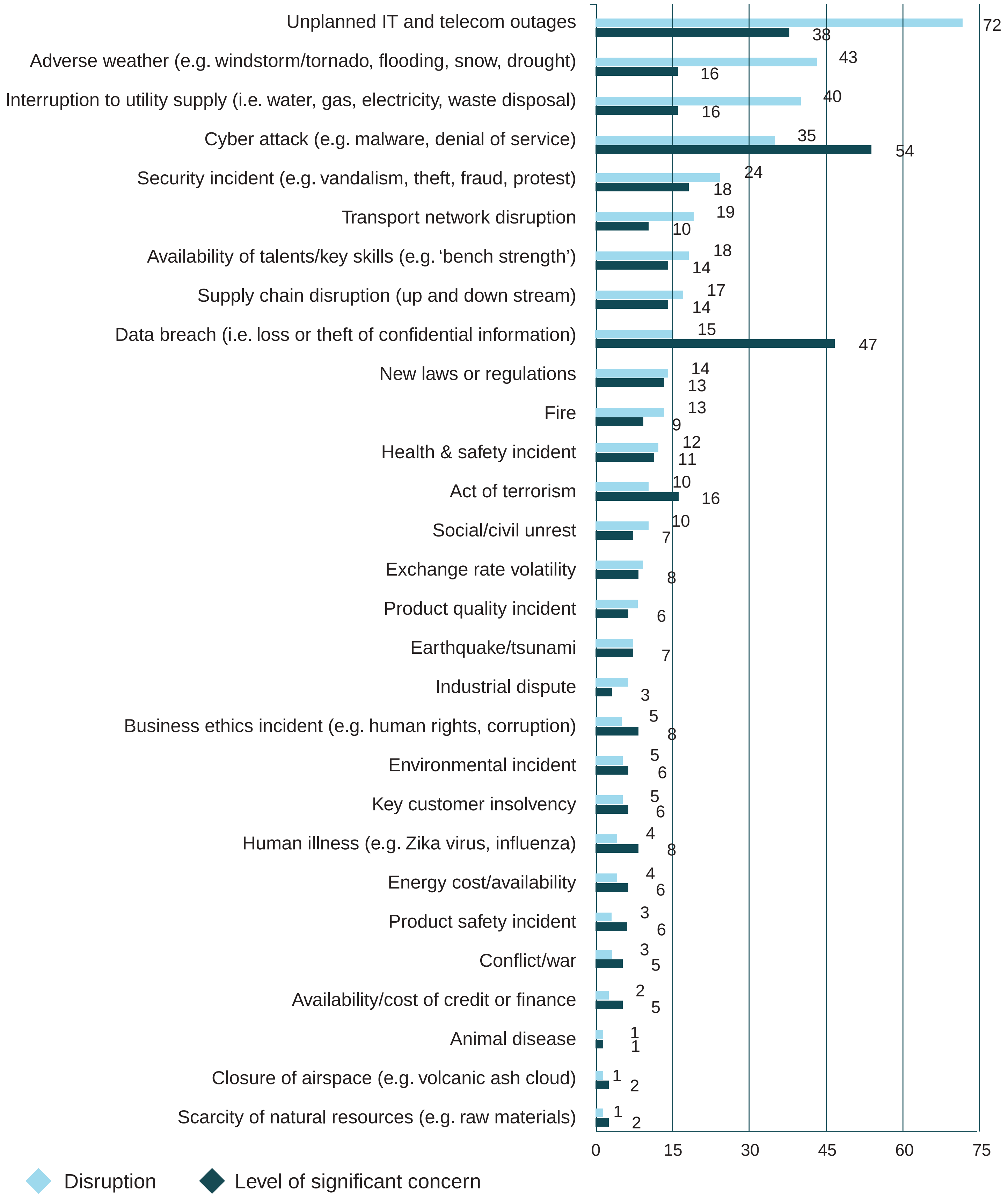


Figure 2. Have you experienced a business disruption due to the following in the last 12 months? (N=602, answers expressed in percentage. Multiple responses allowed)

Case Study:

Worldwide wave of populism affects currency markets

2016 was seen as a year of profound change with a wave of populism sweeping many democracies worldwide. With election outcomes seemingly favouring anti-establishment candidates and policies, it has impacted financial markets and was linked to currency volatility. Some examples are listed below.

- The United Kingdom (UK) voted to leave the European Union (EU) by a narrow margin last June. This led to months of campaigning from both sides and to the resignation of then Prime Minister David Cameron who supported remaining in the EU. The uncertainty triggered by the vote immediately sent the pound down by 8% against the US dollar, its lowest since the 1970s[11]. While the pound has recovered some of its value since then, further falls are expected in the case of a ‘hard Brexit’, which means the UK leaving the EU single market[12] and being liable for tariffs on traded goods and services.
- In the United States, Donald Trump won the presidency last November despite losing the popular vote. This was due to narrow wins in key battleground states that gave him a decisive advantage over his opponent[13]. He beat former US Senator and Secretary of State Hillary Clinton, tipped to win in pre-election polling[14], after a bitterly fought campaign. There are mixed outcomes from a Trump win. The US dollar was momentarily strengthened by his victory, possibly due to a campaign pledge to loosen fiscal policy that might lead to income repatriation in favour of the US[15]. On the other hand, forecasts show how proposed Trump policies might result in significant job losses, slow global growth, and even a ‘trade war’ being more likely[16].
- The result of Italy’s constitutional referendum held in December caused the euro to drop against the US dollar. Italian Prime Minister Matteo Renzi promptly offered his resignation, following through a pledge he made during the referendum campaign, leading to further uncertainty over Italy’s future[17]. This has happened within a context of rising anti European Union movements throughout the continent. The future of the European project may well hang in the balance as the biggest economies in the EU – Germany, France and Italy - will hold general elections, in the next 12 months[18].

[11] http://uk.reuters.com/article/us-britain-markets-sterling-idUKKCN0ZN1R0

[12] https://www.ft.com/content/45ab8f2a-8961-11e6-8cb7-e7ada1d123b1

[13] http://www.bbc.co.uk/news/election-us-2016-37889032

[14] http://uk.businessinsider.com/polls-election-hillary-clinton-donald-trump-2016-11?r=US&IR=T

[15] http://uk.businessinsider.com/us-dollar-after-donald-trump-2016-11?r=US&IR=T

[16] http://money.cnn.com/2016/09/14/news/economy/donald-trump-economic-plan-1-trillion/

[17] http://www.wsj.com/articles/euro-falls-just-slightly-after-italian-exit-polls-show-no-vote-1480891344

[18] http://www.marketwatch.com/story/how-2017-is-likely-to-be-a-turning-point-away-from-the-eurozone-2016-12-14

Emerging trends and uncertainties

Another key metric tracked in the study includes the measurement of practitioner sentiment for emerging trends and uncertainties which may influence organizations in the long run. Among these trends and uncertainties, the use of the internet for malicious attacks (80%) once more comes out on top, mirroring increasing vulnerabilities online. Previous publications such as the BCI Cyber Resilience Report have elaborated on the exploitation of these vulnerabilities by hostile elements and the potential losses it may cause to an organization.

The influence of social media (53%) ranks second which reflects its growing impact on organization's reputation. Reputational damage is being increasingly seen as a consequence of various disruptions such as supply chain incidents, which result in adverse social media attention. The loss of key employee follows at third (50%), which coincides with concern over the availability of key talents and skills on the top 10 of the Horizon Scan.

The prevalence and high adoption of internet dependent services (46%) is fourth in this year's survey, jumping up once place, owing to the increased uptake of cloud platforms especially as a recovery strategy. New regulations and increased regulatory scrutiny (46%) goes down to fifth place. Political change (40%) closely follows in sixth place, up two places. This coincides with a wave of populism sweeping across democracies worldwide, culminating in Brexit, the rise of the populist far-right in countries such as France and Austria, as well as the election of Donald Trump in the United States. Rounding off the top ten are increasing supply chain complexity (seventh at 38%), the potential emergence of a global pandemic (eighth at 36%), changing consumer attitudes and behaviour (ninth at 31%), followed by slow economic growth and its impact on investment (tenth at 30%).

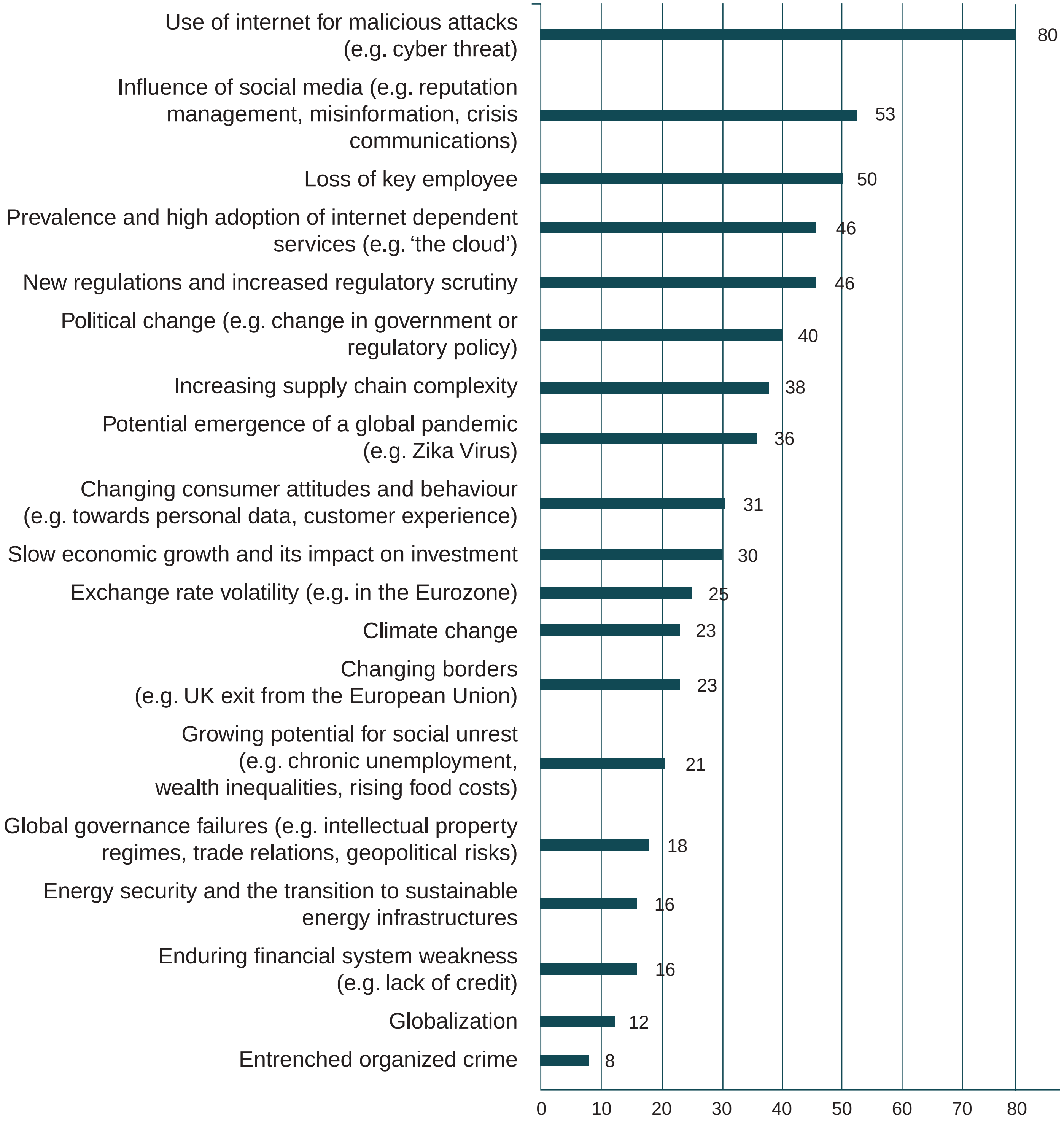


Figure 3. Which of the following trends or uncertainties are on your radar for evaluation in terms of their business continuity implications? (N=637, answers expressed in percentage. Multiple responses allowed.)

A few respondents offered their thoughts on trends and uncertainties that may impact on their organizations.

The full impact of the Brexit vote won’t be seen in the short term. In the UK, I personally believe that, whatever the press says, the unpicking of legislation around EU membership is so horrendously complicated… Far too many people live solely in the world of business and don’t take into account social [trends], economics and the power of the press… The lesson from all of this is… consider whether these would impact your organization if [a particular political outcome] is delivered, and whether there is enough disaffected voters who will accept the message and then help deliver the outcome.

We are concerned as we become more dependent on ‘the cloud’, technology, important third party applications and infrastructure as it relates to our ability to react, strategize and recover from any particular type of vital recipient application incident.

There is a serious economic downturn in Nigeria leading to exchange rate volatility. This impacts [our] ability to import network equipment for delivery of service. There is also a growing wave of terrorism acts in parts of the country that is disrupting operations.

The concentration of processing in global processing centres [leads to increased] concentration of risk. An outage in a location is not limited to a single country anymore but has the potential to disrupt continuity world-wide.

Inordinate delays in financial payments from large government projects to top level vendors creating cascading effects all the way down the supply chain. We may see many small vendors going bankrupt… simply because of cash flow.

Benchmarking longer-term trend analysis

More than two-thirds of organizations (69%) perform a trend analysis (Figure 4). Nonetheless, a quarter of organizations (25%) do not perform this at all, almost unchanged from last year's 26%. This is a worrying development which would require further analysis as to the barriers affecting trend analysis. This also needs attention in terms of industry awareness and advocacy efforts.

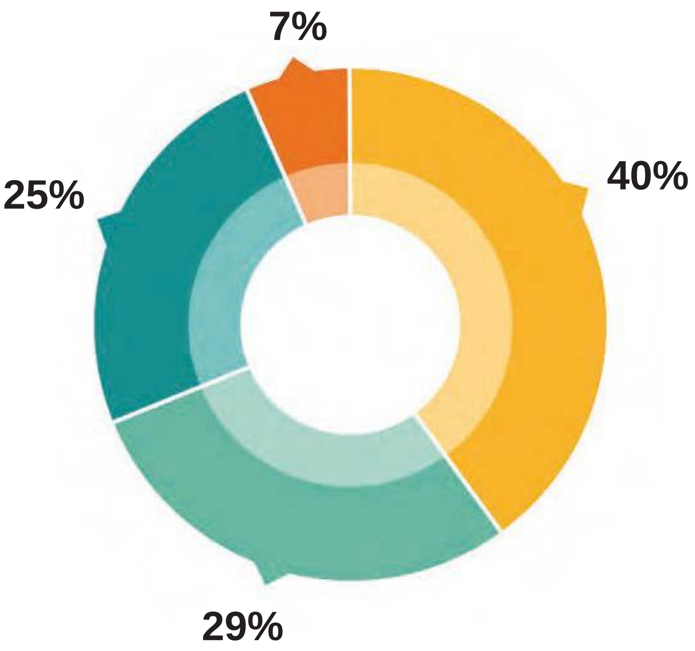


Figure 4. Does your organization conduct longer term trend analysis as part of its horizon scanning activity? (N=655)

Slightly more organizations are aware and draw upon inputs from trend analysis (69%) compared to last year (67%). Nonetheless, almost a third (32%) of respondents still do not have access to trend analysis results or use its findings (Figure 5). This points out to the continued existence of silos within many organizations that act as a barrier to building resilience. Further activity must focus on breaking down these silos within organizations and making trend analysis and similar data freely available to practitioners.

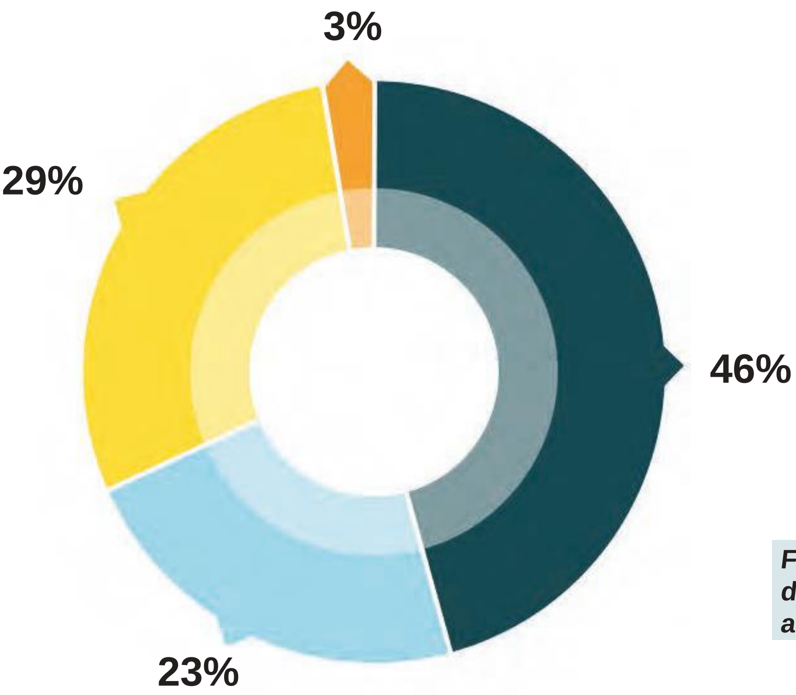


Figure 5. As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme? (N=640)

Respondents share their experiences about conducting trend analysis.

We use a variety of sources [to inform in-house analysis]. The BCI's Horizon Scan Report forms a part of the base of our research.

Part of our organization's continual improvement is the assessment of new scenarios.

The risks identified at a corporate level have little/no direct link to the way we consider business continuity management (BCM). There is scope for a closer link but the risks identified are not operationally focused.

I link the results with our current risks to drive the development of related/up-to-date business continuity plans.

Nearly three-quarters of respondents (73%) will either maintain or increase their investment in business continuity programmes (Figure 6). This may reflect increased awareness of business continuity and its benefits to the organization at large. A recent BCI report elaborates on how business continuity provides value to the organization[20]. Small and medium sized enterprises (SMEs) appear to be willing to maintain business continuity investments, with only 7% proposing budget cuts compared to 16% of large enterprises.

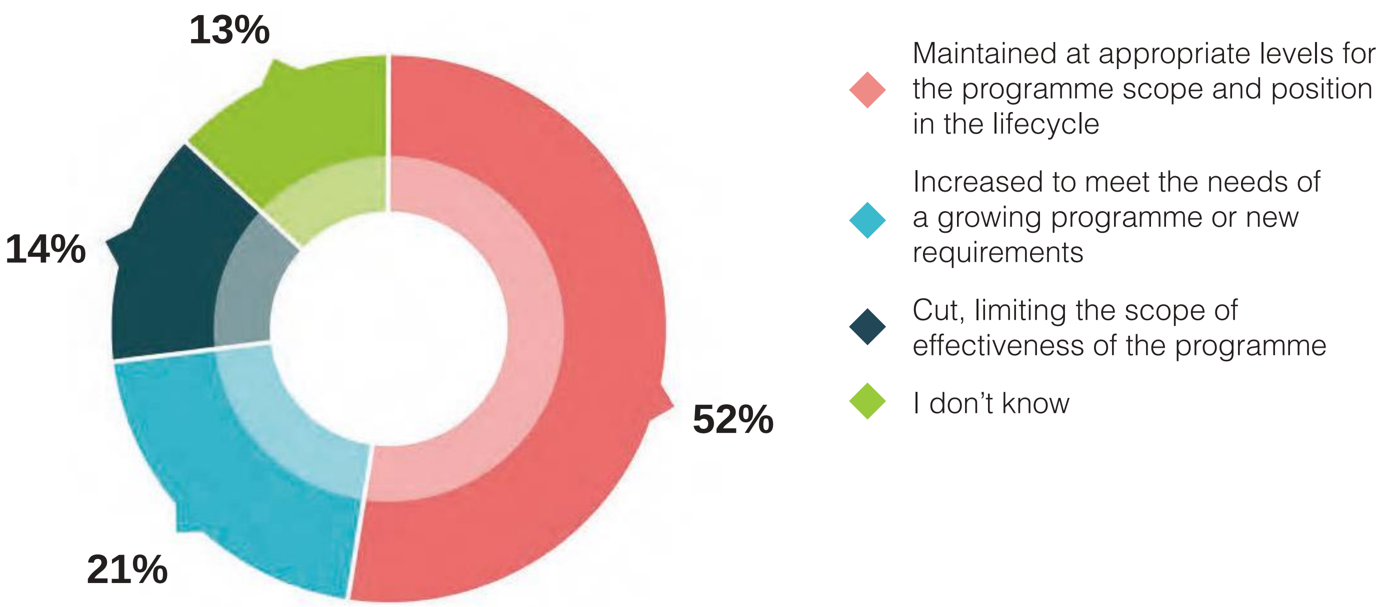


Figure 6. If you have an existing business continuity programme, how will investment levels in 2017 compare to the current year? (N=638)

[20] A copy of the white paper 'Business continuity delivers return on investment' is available here: http://www.thebci.org/index.php/bci-business-continuity-awareness-week-2016-white-paper.

Some respondents offer their thoughts which reflect the challenge for business continuity professionals to get consistent investment.

> Budget justification is the hardest part. The value is evident when business continuity is invoked for real events, but gaining buy-in is always a difficult task.

> A dedicated budget is not allocated and no dedicated department exists [at the moment]. However, more personnel will be included in the business continuity management programme enhancement effort overall [in line] with the ISO standard and BCI Good Practice Guidelines in the future.

> This fiscal year was the first time we attempted to create a specific business continuity budget and next year it will be refined further. Previously it has been 'lost' in other departmental budgets.

ISO 22301 Business Continuity uptake

The uptake of relevant standards such as ISO 22301 remains unchanged with over half of organizations (51%) using the standard in some fashion (Figure 7). This result is unchanged from last year. There is also a decrease in the percentage of organizations not planning to use the standard at all (24% to 18%). Segmenting results among industry sectors reveals that the IT and telecommunications (73%), energy and utility (69%) as well as financial and insurance (68%) sectors register the highest uptake of the ISO 22301 standard. This might be due to increased regulatory scrutiny within these industries.

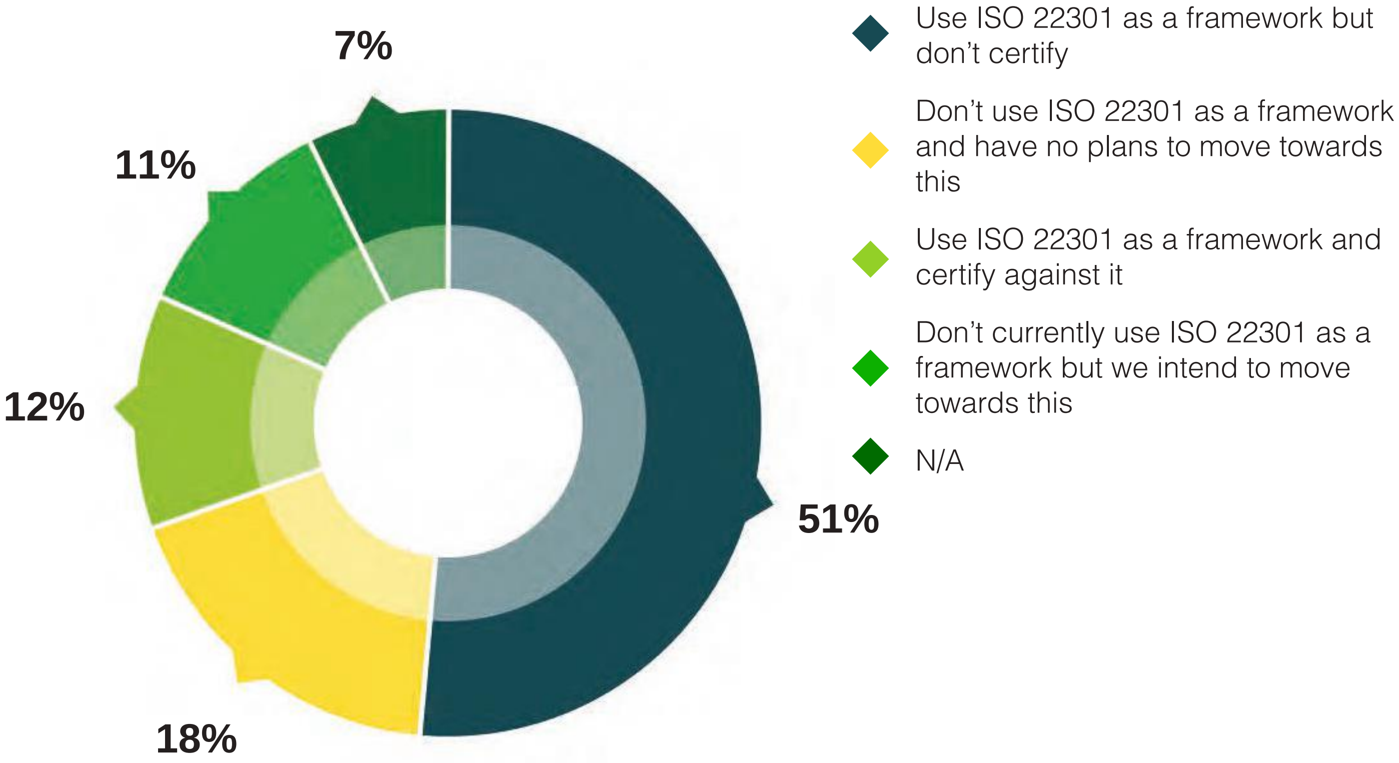


Figure 7. If you have a formal business continuity management programme in place, how does it relate to ISO 22301? (N=707)

3 Conclusion

Horizon scanning is an important exercise as it enables organizations to objectively assess threats which may impact on business performance. Used with trend analysis, horizon scanning is a powerful tool in enabling strategic decision making. As a global study, the BCI Horizon Scan Report benchmarks the perception of various threats and actual disruptions, providing useful data which may complement in-house analytical activity. The following are some of the key insights from this year's BCI Horizon Scan Report.

1 **Organizations need to focus on the objective appraisal of threats and their particular impacts.**

This year's report has highlighted some gaps between the level of concern and actual disruptions caused by various threats. For example, the study noted significantly high levels of concern over cyber attacks and data breach which may be influenced by increased media coverage. Business disruptions nonetheless are still mainly driven by other threats such as unplanned IT and telecom outages and adverse weather. As such, organizations need to continually look at the business impacts of various threats and deploy appropriate tactics to become more resilient.

2 **Cyber issues continue to figure significantly in practitioners' concerns.**

Cyber attacks and data breaches have consistently ranked as the top threats according the BCI Horizon Scan Report in the last three years. This is likely to remain the case moving forward given the development of technologies such as the internet of things and the exponential growth of business data, which may also provide new opportunities for hostile elements to cause disruption. Business continuity plans can help reduce the likelihood and impact of cyber disruptions, allowing organizations to save on costs and maintain brand reputation.

3 **The effects of disruption from adverse weather is a growing concern of many organizations.**

With extreme weather episodes and climate change, effects such as flooding can severely disrupt organizations. Recent research such as the BCI Emergency Communications Report reveal that more than a third (39%) of emergency communications are triggered by adverse weather events. A robust business continuity programme can help in building resilience required to withstand this disruption.

4 **External events underscore the interconnected nature of risks and demonstrate the need for practitioners to include these in planning.**

Business regulation and the overall trading environment may be affected by political events such as Brexit or a significant change in government policy. It is important for organizations to take these into account and plan accordingly.

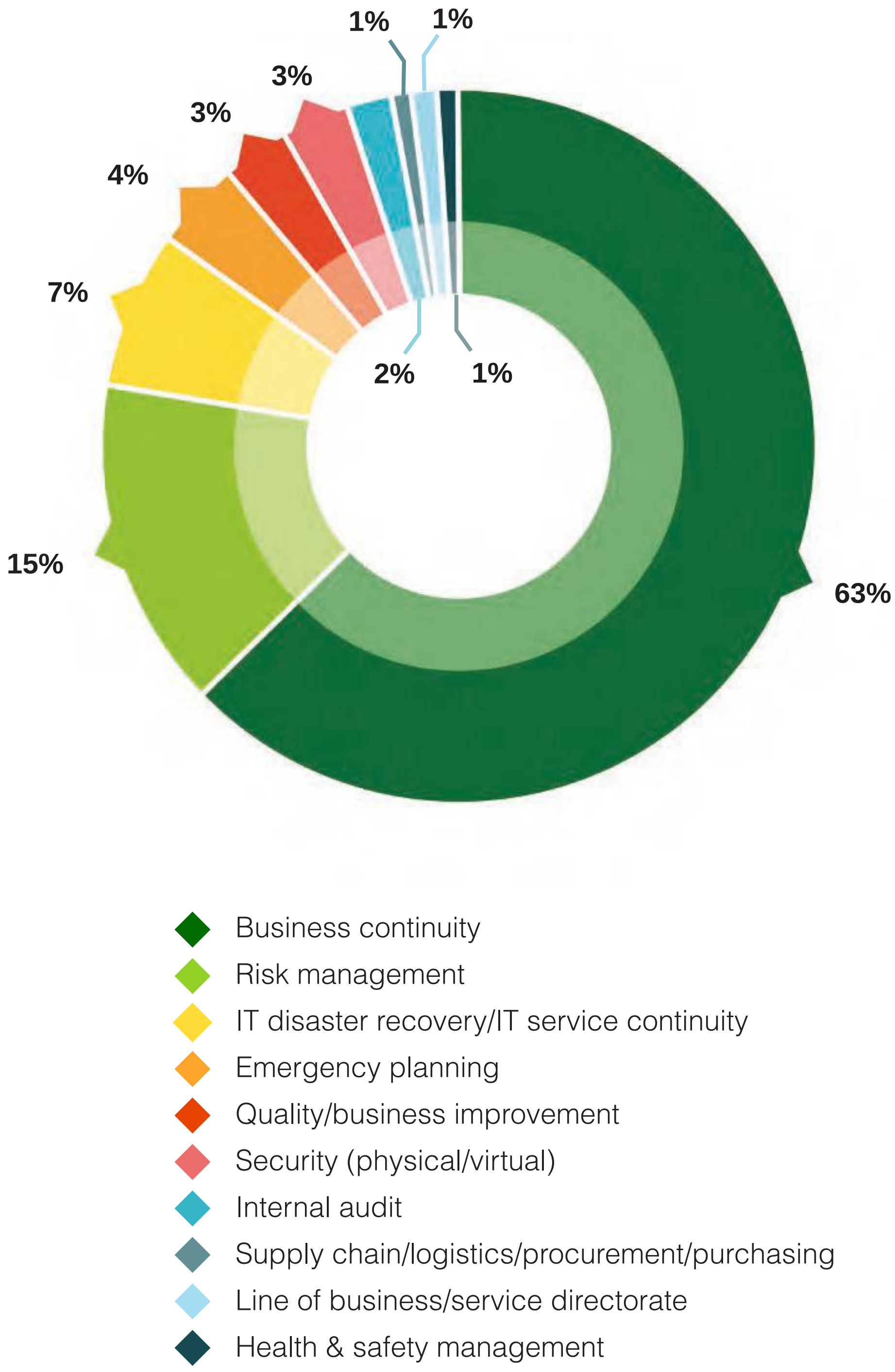
5 **Investments in resilience should be sustained in order for organizations to build and maintain adaptive capacity.**

Recent research such as the BCI white paper on the value of business continuity underscore how investments in this area translate to greater efficiency, lower operational and insurance costs. As such, practitioners are encouraged to build a stronger case for resilience within their organizations by developing their own metrics which show how business continuity and related functions benefit the bottom line.

5 | Annex

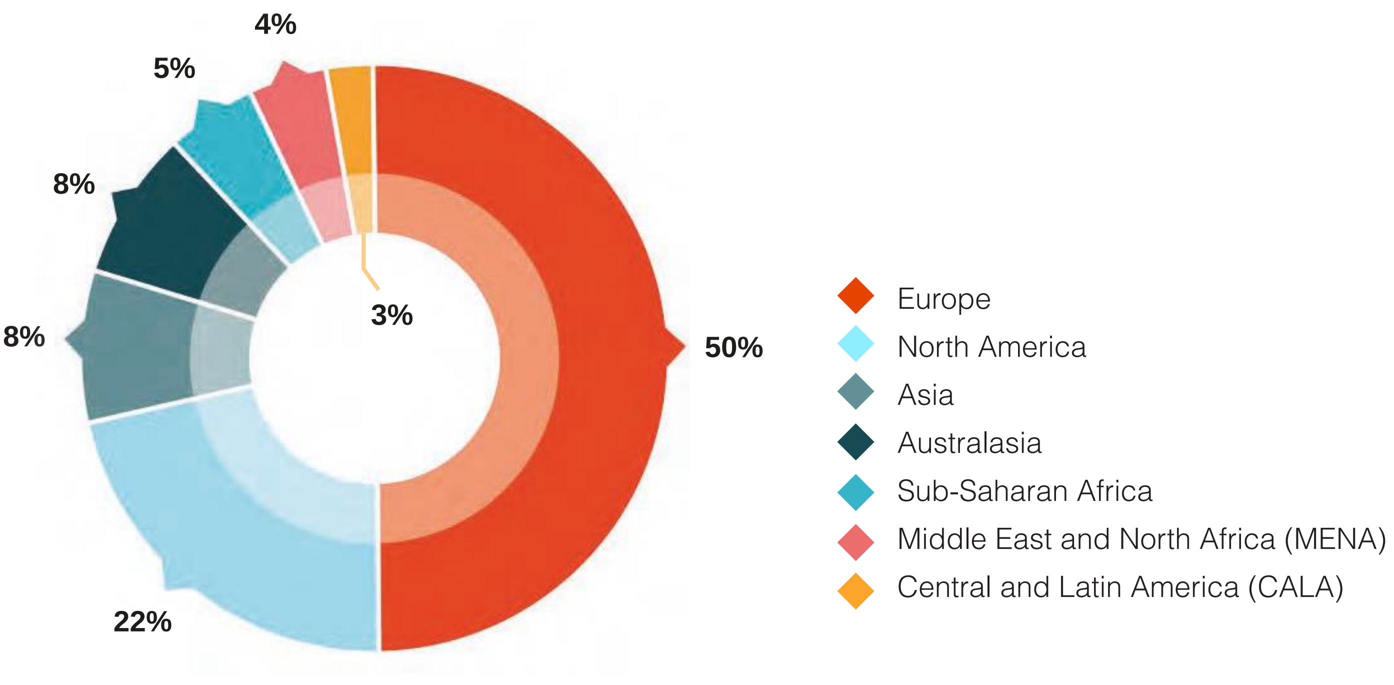
1. Demographic information

a. Functional role of the respondents



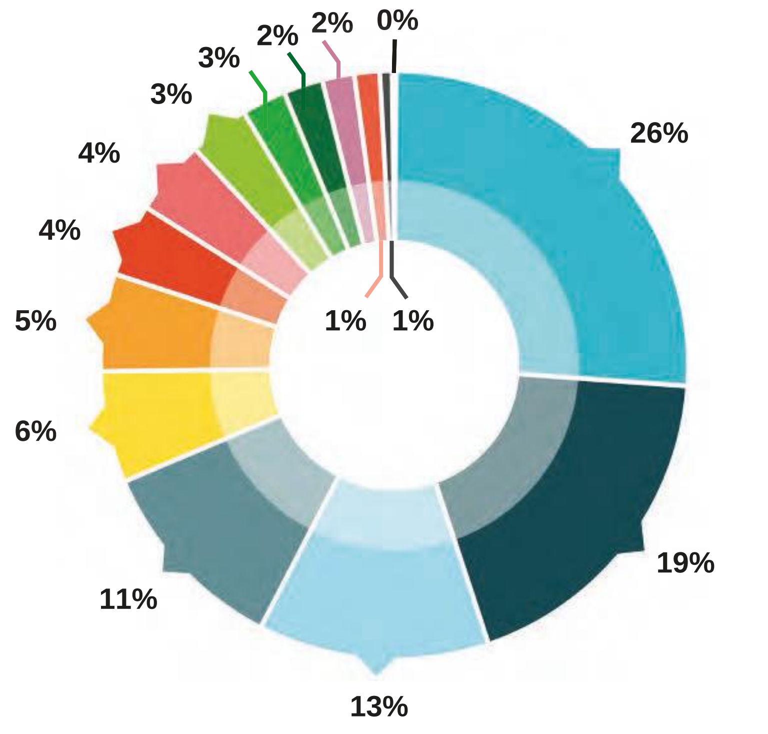
Which of the following best describes your functional role? (Numbers are expressed as percentage, N=726)

b. Geographical base



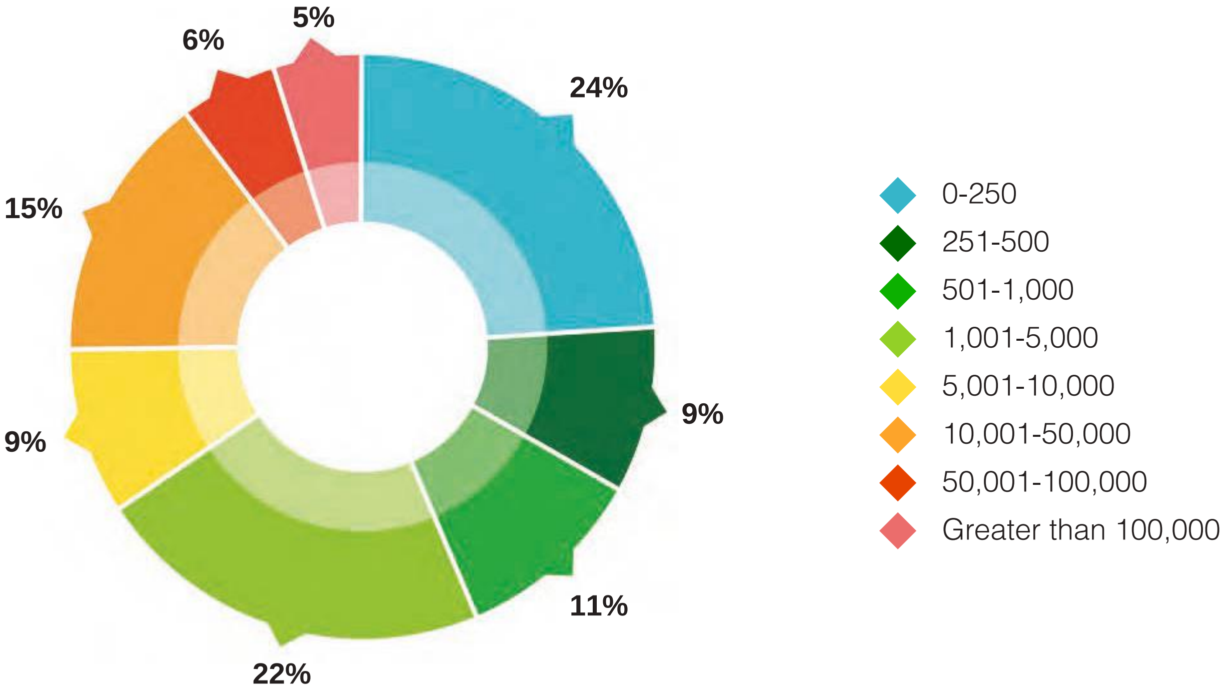
Country/region (N=726).

c. Industry sector



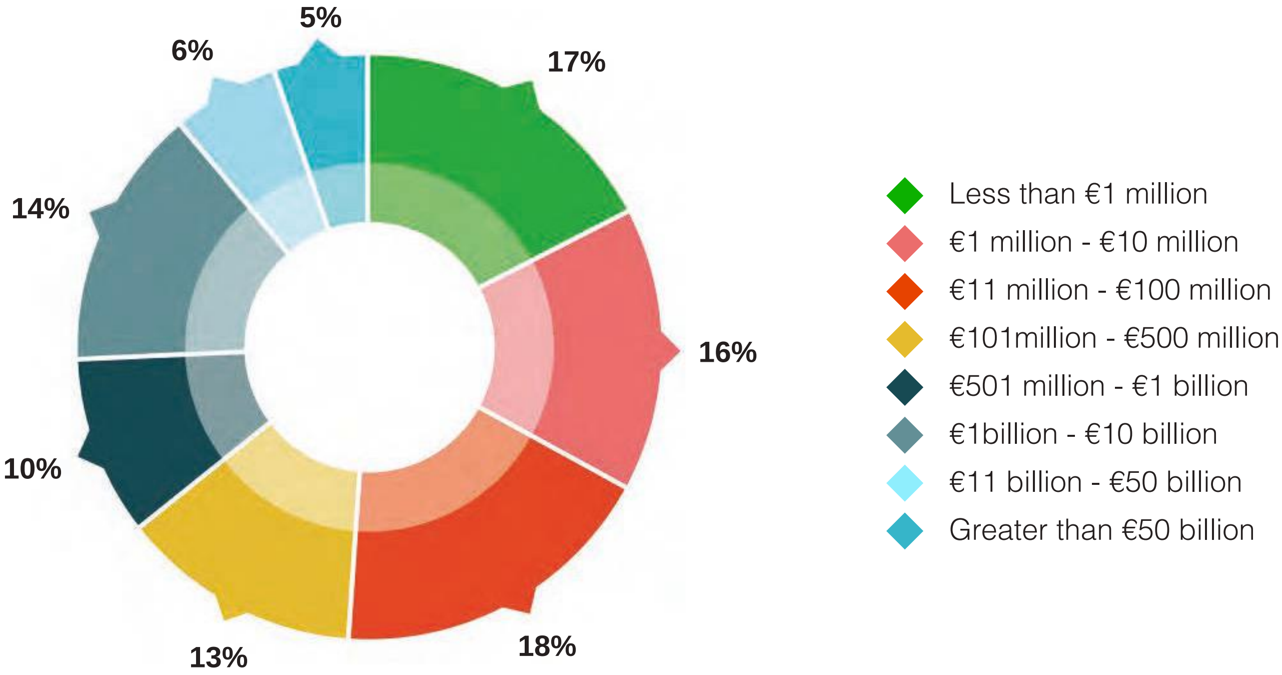
Industry sector (N=726)

d. Number of employees



Number of employees (N=726)

e. Approximate annual turnover



Annual turnover (N=726)

2. Comparison by region / country

	Europe	North America	Asia	Australasia
Top three threats	Cyber attack (53%) Data breach (41%) Unplanned IT & telecom outages (36%)	Data breach (59%) Cyber attack (58%) Unplanned IT & telecom outages (40%)	Cyber attack (56%) Data breach (50%) Unplanned IT & telecom outages (46%)	Data breach (50%) Cyber attack (46%) Unplanned IT & telecom outages (39%)
Top three disruptions	Unplanned IT & telecom outages (77%) Cyber attack (38%) Interruption to utility supply (38%)	Unplanned IT & telecom outages (71%) Adverse weather (67%) Cyber attack (37%)	Unplanned IT & telecom outages (55%) Adverse weather (36%) Interruption to utility supply (28%)	Unplanned IT & telecom outages (84%) Adverse weather (52%) Interruption to utility supply (50%)
Top three trends	Use of internet for malicious attacks (82%) Influence of social media (57%) Loss of key employee (53%)	Use of internet for malicious attacks (80%) Influence of social media (48%) Prevalence and high adoption of Internet dependent services (48%)	Use of internet for malicious attacks (70%) Potential emergence of a global pandemic (54%) New regulations and increased regulatory scrutiny (50%)	Use of internet for malicious attacks (84%) Prevalence and high adoption of internet dependent services (63%) Influence of social media (58%)
Conducting Trend Analysis	73%	66%	56%	71%
Use of ISO 22301	67%	53%	59%	74%
Level of BC investment	Up 17% Down 14% Unchanged 54%	Up 25% Down 12% Unchanged 50%	Up 24% Down 18% Unchanged 48%	Up 13% Down 2% Unchanged 74%

2. Comparison by region / country

	Middle East & North Africa	Central & Latin America	Sub-Saharan Africa	UK
Top three threats	Cyber attack (60%) Unplanned IT & telecom outages (36%) Data breach (36%)	Cyber attack (39%) Business ethics (33%) New laws or regulations (33%)	Cyber attack (63%) Unplanned IT & telecom outages (53%) Exchange rate volatility (50%)	Cyber attack (53%) Data breach (41%) Unplanned IT & telecom outages (36%)
Top three disruptions	Use of internet for malicious attacks (81%) Loss of key employee (52%) Increasing supply chain complexity (48%)	New regulations and increased regulatory scrutiny (53%) Use of internet for malicious attacks (53%) Loss of key employee (53%)	Use of the internet for malicious attacks (84%) Political change (71%) Slow economic growth and its impact on investment (68%)	Use of internet for malicious attacks (83%) Influence of social media (58%) Loss of key employee (55%)
Top three trends	Use of internet for malicious attacks (81%) Loss of key employee (52%) Increasing supply chain complexity (48%)	New regulations and increased regulatory scrutiny (53%) Use of internet for malicious attacks (53%) Loss of key employee (53%)	Use of the internet for malicious attacks (84%) Political change (71%) Slow economic growth and its impact on investment (68%)	Use of internet for malicious attacks (83%) Influence of social media (58%) Loss of key employee (55%)
Conducting Trend Analysis	59%	58%	78%	74%
Use of ISO 22301	45%	61%	71%	69%
Level of BC investment	Up 30% Down 11% Unchanged 44%	Up 25% Down 25% Unchanged 25%	Up 42% Down 16% Unchanged 35%	Up 17% Down 13% Unchanged 55%

2. Comparison by region / country

	US	Canada	Australia	Netherlands
Top three threats	Data breach (60%) Cyber attack (59%) Unplanned IT & telecom outages (41%)	Data breach (57%) Cyber attack (53%) Unplanned IT & telecom outages (37%)	Cyber attack (56%) Data breach (54%) Unplanned IT & telecom outages (38%)	Cyber attack (63%) Data breach (58%) Unplanned It & telecom outages (26%)
Top three disruptions	Unplanned IT and telecom outages (76%) Adverse weather (68%) Cyber attack (37%)	Adverse weather (64%) Unplanned IT and telecom outages (57%) Interruption to utility supply (43%)	Unplanned IT and telecom outages (89%) Adverse weather (53%) Interruption to utility supply (53%)	Unplanned IT and telecom outages (82%) Cyber attack (53%) Act of terrorism (35%)
Top three trends	Use of internet for malicious attacks (81%) Prevalence and high adoption of internet dependent services (51%) Influence of social media (49%)	Use of internet for malicious attacks (76%) Loss of key employee (48%) Influence of social media (45%)	Use of internet for malicious attacks (87%) Prevalence and high adoption of internet dependent services (66%) Influence of social media (63%)	Use of internet for malicious attacks (88%) Influence of social media (65%) New regulations and increased regulatory scrutiny (53%)
Conducting Trend Analysis	66%	70%	70%	79%
Use of ISO 22301	51%	59%	72%	57%
Level of BC investment	Up 26% Down 13% Unchanged 50%	Up 21% Down 10% Unchanged 52%	Up 10% Down 3% Unchanged 82%	Up 26% Down 11% Unchanged 53%

2. Comparison by region / country

	South Africa	Italy	Belgium	India
Top three threats	Cyber attack (58%) Unplanned IT & telecom outages (42%) Data breach (42%)	Cyber attack (29%) Data breach (29%) Availability of talent/ key skills (24%)	Cyber attack (82%) Unplanned IT and telecom outages (71%) Act of terrorism (53%)	Cyber attack (41%) Unplanned IT and telecom outages (41%) Data breach (41%)
Top three disruptions	Interruption to utility supply (68%) Security incident (63%) Unplanned IT and telecom outages (63%)	Interruption to utility supply (47%) Adverse weather (40%) Unplanned IT and telecom outages (33%)	Unplanned IT and telecom outages (88%) Cyber attack (76%) Act of terrorism (59%)	Adverse weather (56%) Social/civil unrest (44%) Unplanned IT and telecom outages (37%)
Top three trends	Use of internet for malicious attacks (83%) Political change (72%) Slow economic growth and its impact on investment (72%)	Use of internet for malicious attacks (81%) Loss of key employee (62%) New regulations and increased regulatory scrutiny (56%)	Prevalence and high adoption of internet dependent services (82%) Use of internet for malicious attacks (82%) Influence of social media (71%)	Use of internet for malicious attacks (56%) Growing potential for social unrest (56%) New regulations and increased regulatory scrutiny (56%)
Conducting Trend Analysis	68%	56%	70%	53%
Use of ISO 22301	58%	53%	73%	74%
Level of BC investment	Up 39% Down 22% Unchanged 28%	Up 27% Down 7% Unchanged 47%	Up 12% Down 18% Unchanged 71%	Up 37% Down 19% Unchanged 31%

3. Comparison by industry sector

	Financial & Insurance	Professional services	Public administration & defence	IT & Communications
Top three threats	Cyber attack (65%) Data breach (61%) Unplanned IT and telecom outages (46%)	Cyber attack (50%) Data breach (44%) Unplanned IT and telecom outages (34%)	Cyber attack (49%) Data breach (35% Unplanned IT and telecom outages (29%)	Cyber attack (68%) Data breach (56%) Unplanned IT and telecom outages (53%)
Top three disruptions	Unplanned IT and telecom outages (76%) Cyber attack (44%) Adverse weather (44%)	Unplanned IT and telecom outages (70%) Interruption to utility supply (32%) Adverse weather (28%)	Unplanned IT and telecom outages (78%) Interruption to utility supply (52%) Adverse weather (45%)	Unplanned IT and telecom outages (78%) Cyber attack (48%) Interruption to utility supply (39%)
Top three trends	Use of internet for malicious attacks (83%) New regulations and regulatory scrutiny (59%) Influence of social media (53%)	Use of internet for malicious attacks (79%) Prevalence and high adoption of internet dependent services (57%) Loss of key employee (55%)	Use of internet for malicious attacks (82%) Influence of social media (64%) Loss of key employee (57%)	Use of internet for malicious attacks (91%) Loss of key employee (53%) Prevalence and high adoption of internet dependent services (53%)
Conducting Trend Analysis	81%	55%	67%	68%
Use of ISO 22301	68%	60%	66%	73%
Level of BC investment	Up 24% Down 7% Unchanged 59%	Up 19% Down 6% Unchanged 57%	Up 15% Down 21% Unchanged 50%	Up 26% Down 12% Unchanged 54%

3. Comparison by industry sector

	Health & social care	Manufacturing	Retail & Wholesale	Energy & Utility services
Top three threats	Data breach (42%) Cyber attack (39%) Unplanned telecom and IT outages (34%)	Cyber attack (38%) Supply chain disruption (30%) Unplanned It and telecom outages (27%)	Cyber attack (40%) Supply chain disruption (30%) Data breach (30%)	Cyber attack (58%) Data breach (50%) Unplanned IT and telecom outages (37%)
Top three disruptions	Unplanned IT and telecom outages (65%) Adverse weather (56%) Interruption to utility supply (53%)	Unplanned IT and telecom outages (60%) Supply chain disruption (60%) Adverse weather (51%)	Unplanned IT and telecom outages (75%) Adverse weather (71%) Supply chain disruption (50%)	Adverse weather (53%) Unplanned IT and telecom outages (53%) Interruption to utility supply (37%)
Top three trends	Use of internet for malicious attacks (66%) Potential emergence of a global pandemic (49%) New regulations and increased regulatory scrutiny (49%)	Increasing supply chain complexity (58%) Use of internet for malicious attacks (58%) Changing consumer attitudes and behaviour (47%)	Use of internet for malicious attacks (85%) Increasing supply chain complexity (74%) Influence of social media (67%)	Use of internet for malicious attacks (87%) Influence of social media (65%) New regulations and increased regulatory scrutiny (61%)
Conducting Trend Analysis	75%	75%	63%	82%
Use of ISO 22301	59%	58%	55%	69%
Level of BC investment	Up 14% Down 31% Unchanged 37%	Up 17% Down 22% Unchanged 50%	Up 14% Down 25% Unchanged 46%	Up 30% Down 17% Unchanged 52%

4. Comparison by business size

	Small and medium sized enterprises (SMEs)	Large enterprises
Top three threats	Cyber attack (45%) Data breach (37%) Unplanned IT and telecom outages (36%)	Cyber attack (57%) Data breach (49%) Unplanned IT and telecom outages (39%)
Top three disruptions	Unplanned IT and telecom outages (66%) Interruption to utility supply (36%) Adverse weather (26%)	Unplanned IT and telecom outages (74%) Adverse weather (48%) Interruption to utility supply (40%)
Top three trends	Use of internet for malicious attacks (76%) Los of key employee (53%) New regulations and increased regulatory scrutiny (52%)	Use of internet for malicious attacks (81%) Influence of social media (55%) Loss of key employee (49%)
Conducting Trend Analysis	55%	73%
Use of ISO 22301	59%	65%
Level of BC investment	Up 19% Down 7% Unchanged 55%	Up 21% Down 16% Unchanged 52%

About the Authors

Patrick Alcantara DBCI (BCI Senior Research Associate) wrote this report. He heads the research department of the BCI. 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 CBCI (BCI Research Assistant) co-authored this report and case studies. He also wrote the Annex of this report. He has a Masters in Geopolitics, Territory and Security (Merit) from King's College London. He has experience writing academic and industry publications, speaking at international conferences, and delivering projects for companies such as Zurich, Regus, and Transputec. 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

The BCI would like to thank BSI for sponsoring this research for the sixth consecutive year. We also acknowledge Kaara Pallop (BSI Global Portfolio Manager) for her assistance during the survey period. Andrew Scott CBCI (Senior Communications Manager, BCI) directed promotions during and after the study, as well as 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.

Contact BSI

Learn more
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 February 2017