Business Continuity Institute

HORIZON SCAN REPORT 2018

Correct as of January 2018

bsi.

Foreword
Business Continuity Institute

In its seventh edition, with the support of BSI, the BCI Horizon Scan Report 2018 presents findings on what the main threats are to organizations, how professionals perceive them, and what measures they are adopting to counter them. The report has now become a highly regarded source of information for business continuity and resilience experts, who rely on it to shape their strategies.

This year, the threat landscape has proved to be incredibly complex and varied. Non-physical threats remain at the top of the list with large scale cyber attacks such as WannaCry and NotPetya that are now much more likely to disrupt operations than in the past.

However, professionals are also concerned about physical disruptions, which can undermine employees' safety and cause significant financial damage. Whether it is a hurricane that cuts off the power supply or an active shooter incident (such as a terrorist attack) that causes a building lockdown, organizations need to be ready. Looking at the past twelve months, the devastation caused by hurricanes Harvey in the US and Vinta in the Philippines but also the persistent threat of terrorism across several regions are clear examples of why preparedness is key to survival and success.

This report also highlights how imminent certain threats are perceived to be compared to their actual disruption levels. Worryingly, findings reveal that events such as pandemics tend to slip out of the radar, despite warnings from experts. This shows once again the importance of horizon scanning exercises that can provide experts with a clear picture of what challenges lie ahead.

On the bright side, business continuity arrangements feature as one of the most relevant type of arrangements to build resilient organizations. This is a trend that has increased over the years, with a growing adoption of both plans and industry standards. In addition, a new metric added to the report this year for the first time reveals how the longer organizations adopt business continuity for, the likelier they are to keep investing in it, which is probably due to the long term benefits this function brings.

Embedding business continuity and sharing the results of horizon scanning analysis with professionals from various disciplines (such as risk, physical security or disaster recovery) is key to building resilience. This report aims to show why this is the case and to raise awareness among professionals from several regions, sectors and industry roles.

David Thorp
Executive Director, BCI

Foreword
BSI

The BCI Horizon Scan report 2018 is a great example of building a robust partnership to provide collective insight and market analytics to support organizations. BSI has been partnering with the BCI for over 7 years to produce this report, helping organizations understand the business environment in which we all operate.

The business world has changed significantly since the report launched, yet there is remarkable consistency to the top business threats. Whilst the pace of technology development moves at lightning speed, the role it plays in society and how it supports business simply becomes more fundamental. So it's no surprise cyber-attacks, data breaches and unplanned IT outages remain the top threats – if these threats are exposed, the impact can be significant to operations and ultimately reputations. We saw a number of examples hit the headlines in 2017 from healthcare organizations to financial service firms, bringing these threats closer to home and making it real.

With the stakes continuing to rise and the continual development of more sophisticated smart technologies, organizations can't afford to be complacent.

Business continuity continues to be of primary importance for most organizations. For the third year running the use of ISO 22301 continues to increase with 70% of survey respondents now actively using the standard. Coupled with the growth in BCM investment, it's clear to see the importance being placed on preparing an organization.

But it isn't just business continuity that is essential to building a resilient organization - a much more holistic approach, one that enables you to understand indicative strengths and vulnerabilities, is required.

In 2017 BSI launched the world's first Organizational Resilience Index. Derived from four standards of best practice it outlines 16 key elements of resilience that we asked over 1260 senior decision makers to rank their perceived performance and importance of each element.

There are real synergies between the results of this report and the senior executive rankings against these elements in relation to both performance and importance. Executives considered all elements to be important, but reputational risk was perceived as the most important of all. The increase in investments in continuity planning and the continued engagement from business continuity professionals demonstrates recognition of trend analysis and scanning as a contributor to protecting reputations.

Howard Kerr
BSI Chief Executive

Contents

1 Executive Summary

Executive Summary

657
respondents

76
countries

Top 10 threats

2
Data breach

3
Unplanned IT and telecom outages

4
Interruption to utility supply

5
Adverse weather

6
Act of terrorism

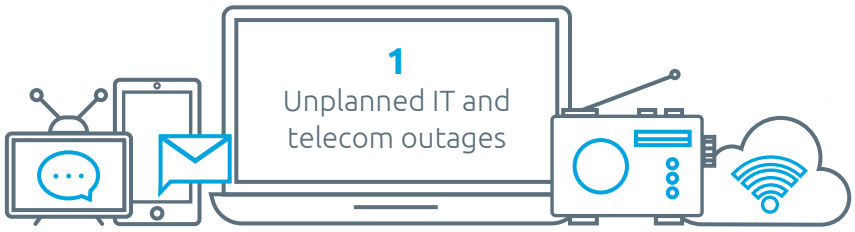
7
Security incident

8
Fire

9
Supply chain disruption

10
Transport network disruption

Top 10 disruptions

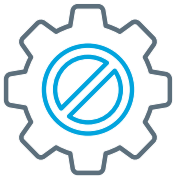


1
Unplanned IT and telecom outages

2
Adverse weather

3
Interruption to utility supply

4
Cyber attack



5
Availability of talents/key skills

6
Security incident

7
Transport network disruption

8
New laws or regulations

9
Fire

10
Supply chain disruption

Top 10 trends

2
Loss of key employee

3
Influence of social media

4
New regulations and increased regulatory scrutiny

5
Prevalence and high adoption of internet dependent services

6
Political change

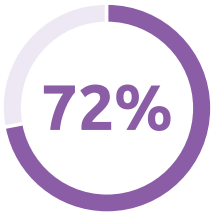
7
Potential emergence of a global pandemic

8
Increasing supply chain complexity

9
Changing consumer attitudes and behavior

10
Climate change

Trend analysis:

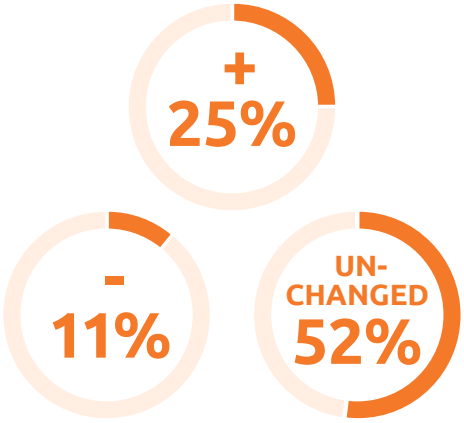


of respondents conduct longer term trend analysis as part of their horizon scanning activity

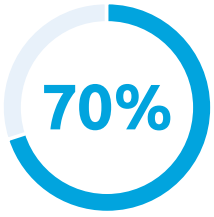
BUT

do not have access to this information

Investment levels



ISO 22301 uptake



of respondents use ISO 22301

2 Main report

Introduction

For the seventh consecutive year, with the support of BSI, the BCI Horizon Scan report 2018 presents findings on business threats in the near and longer term. The report also benchmarks how organizations prepare for disruptions, looking at the uptake of business continuity arrangements.

This report has now become a valuable resource to professionals working in business continuity and organizational resilience. The methodology involved a survey that included 657 respondents from 76 countries, as well as relevant case studies.

Measuring concern over specific threats

Cyber threats continue to be the top concern for business continuity and resilience professionals. Cyber attacks head the chart, as 53% of the respondents are "extremely concerned" about them (Figure 1). Data breach (42%) and unplanned IT or telecom outages (36%) rank second and third, completing the top three. Looking at the past twelve months, with attacks such as WannaCry and NotPetya, it is easy to see why non-physical threats are such a concern.

On the other hand, physical security remains a strong concern too for organizations. Interruption to utility supply and adverse weather (18%) are considered as the fourth and fifth main threats by professionals. These two concerns can often be connected to each other, for example severe weather events, such as hurricanes Irma and Harvey, saw people being cut off from basic services.

Security incidents (16%) dropped by two positions but still remains firmly in the top ten, as joint sixth with acts of terrorism. This reflects a clear concern by respondents towards workplace violence. Previous BCI research shows how a growing number of organizations are adopting measures to build effective emergency communications responses to this type of incident[1].

Fire (14%) ranks as eighth; incidents such as the Grenfell Tower fire might be the reason for such concern rising into the top ten. Finally, supply chain (13%) and transport network disruptions (13%) rank as ninth and tenth, possibly due to the rising threat of physical disruptions. Indeed, further BCI research shows how terrorism is one of the top ten concerns for professionals dealing with supply chains[2].

1 BCI Emergency Communications Report 2017.

2 BCI Supply Chain Resilience Report 2017.

It is worth noting how challenges such as new laws or regulations (12%) and the availability of key talent/skills (11%) drop to the eleventh and thirteenth positions (from last year's ninth and tenth). In light of the current global wave of political uncertainty as well as the approaching implementation date of the European General Data Protection Regulation (GDPR), it is interesting to observe that organizations devote more attention to different types of threats.

Year	Top five threats
2016	**1.** Cyber attack **2.** Data breach **3.** Unplanned IT & telecom outages **4.** Act of terrorism **5.** Security incident
2017	**1.** Cyber attack **2.** Data breach **3.** Unplanned IT & telecom outages **4.** Security incident **5.** Adverse weather
2018	**1.** Cyber attack **2.** Data breach **3.** Unplanned IT & telecom outages **4.** Interruption to utility supply **5.** Adverse weather

Table 1. Top threats to organizations through the years.

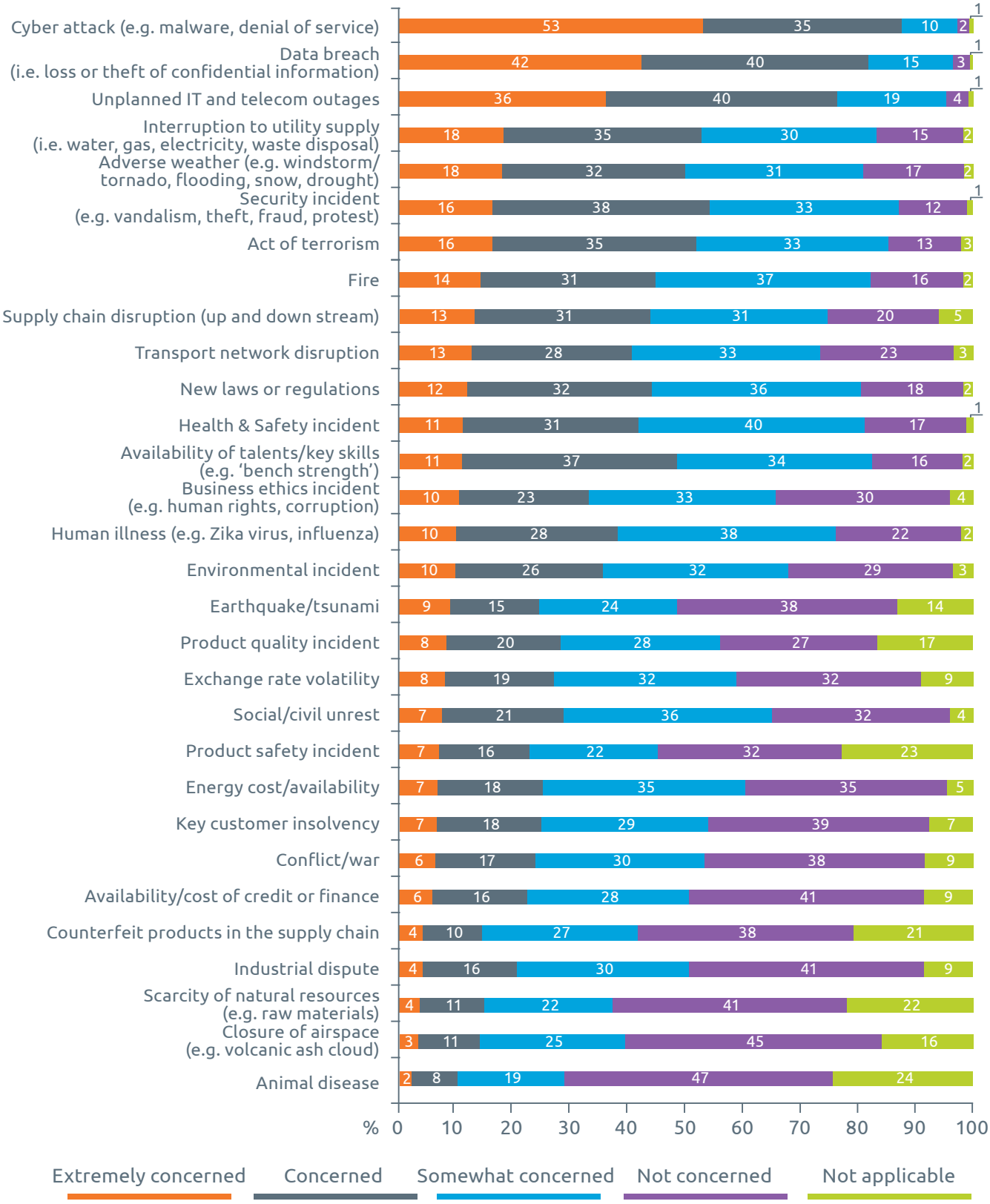


Figure 1. Based on your analysis, how concerned are you about the following threats to your organization in 2018? (N=595, answers expressed in percentage. Multiple responses allowed.)

Case study

Pandemics

In the last forty years, the number of pandemics has increased threefold. Experts have already identified what could be the next outbreak – a bird flu that is spreading across China and is referred to as H7N9. The virus causes severe problems to the respiratory system, with a high percentage of those infected ending up in intensive care. This is only the last of a number of deadly diseases that have spread in the last few years, from Ebola in West Africa to the Zika virus in South America, and the threat is not likely to decrease in the future[3]. In addition, future health emergencies could also be man-made. Experts have pointed out that terrorist organizations might try to acquire biological weapons to spread infections on a large scale. While this remains an unlikely scenario at the moment, terrorist groups such as the Islamic State (IS) have proved willing to conduct this type of attack[4].

Both national governments and international organizations are aware of the threat and are formulating guidelines and advice to prepare for health emergencies. Business continuity plans are considered a pivotal part of response plans, as they can help organizations ensure the safety of their staff and the continuity of operations.

The World Health Organizations (WHO) states that business continuity plans "are at the heart of preparing all levels and groups of society for an emergency". In a document on pandemics, the WHO outlines the main actions to take when it comes to handling a health crisis[5]. The Australian government also provides a template for a "Pandemic Management plan", as part of a business continuity plan[6]. The Canadian public sector too has produced specific guidelines for a business continuity plan for health hazards. This is different from a regular plan since it focuses more on the human resources available during a crisis (as these might be more affected) rather than physical property such as buildings or data[7].

Having a plan tailored to pandemics is key to facing what is considered one of the great challenges of the future. Applying insights from horizon scanning analyses will also help professionals make an informed decision to understand how vulnerable an organization is when facing this particular threat.

3 http://time.com/magazine/us/4766607/may-15th-2017-vol-189-no-18-u-s/

4 https://www.reuters.com/article/us-biological-weaons-commentary/commentary-the-next-super-weapon-could-be-biological-idUSKBN17L1SZ

5 http://www.who.int/influenza/preparedness/pandemic/PIRM_withCoverPage_201710_FINAL.pdf?ua=1

6 https://www.tisn.gov.au/Documents/Template+for+Pandemic+Plan.pdf

7 https://www.ccohs.ca/publications/PDF/businesscontinuity.pdf

Measuring actual disruption levels

For the second year, the BCI Horizon Scan shows how disruptions compare to levels of concern over specific threats (as expressed in figure 1). This chart aims to show how the perception of certain disruptions might differ from their impact, making the case for why risk assessments should be part of a business continuity programme. (Figure 2).

The top three disruptions according to respondents are unplanned IT and telecommunications outages (67%), adverse weather (50%) and interruption to utility supply (43%). It is interesting to see that cyber attacks only rank fourth (37%) when it comes to measuring disruptions, while they are the number one concern for professionals. This is consistent with last year's results and it might be due to the fact that cyber attacks can have a very high impact even if striking occasionally, as shown by the WannaCry ransomware campaign that managed alone to affect several organizations worldwide. Availability of key talent/skills (22%) completes the top five, despite not being one of the top ten concerns for professionals.

Further down the chart, ranking sixth and seventh, security incidents (20%) and transport network disruption (18%) match the level of concern over physical security expressed by organizations. Previous BCI research on emergency communications also reveals security related issues to be the among the most disruptive ones[8].

It is interesting to see that new laws or regulations (16%) are considered the eighth most common disruption, even though they are not considered one of the top ten concerns. This could be an opportunity to evaluate and improve processes, since failing to make the necessary arrangements for a new piece of legislation, such as GDPR, could be extremely disruptive for an organization.

Fire (16%), supply chain disruption (14%) and health and safety incidents (13%) round up the top ten, consistent with the level of concern respondents showed about these threats.

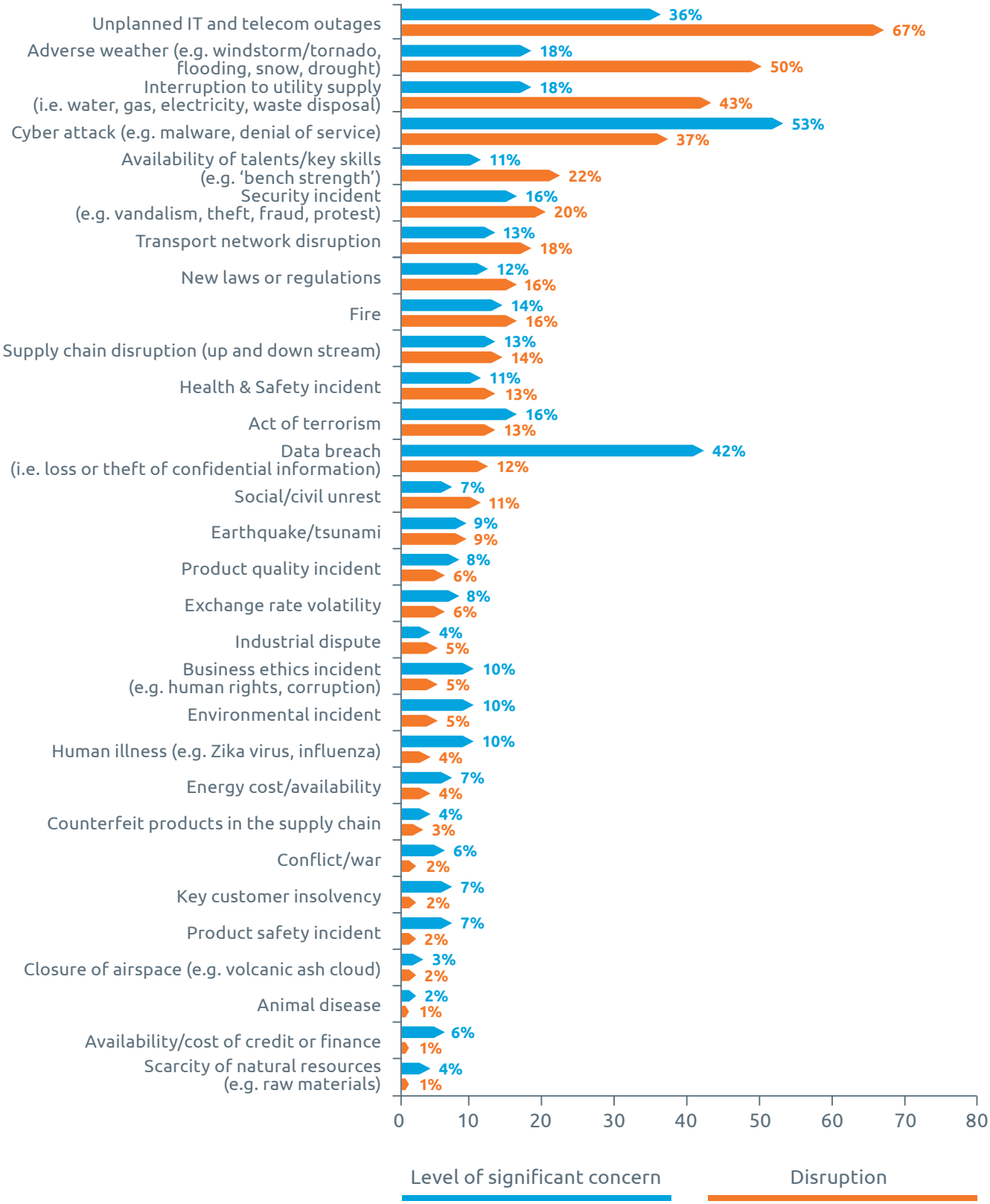


Figure 2. Have you experienced a business disruption due to the following in the last 12 months? (N=538, answers expressed in percentage. Multiple responses allowed.)

Emerging trends and uncertainties

The report also measures emerging trends and uncertainties in the longer term[9] (Figure 3). The use of the internet for malicious attacks (77%) remains the number one threat, consistent with previous findings in this report. Indeed, with the increasing adoption of Internet of Things (IoT) devices, it is likely that cyber threats will intensify in the foreseeable future. Loss of key employee (51%) and influence of social media (50%) rank second and third, swapping places from last year. The top five is then completed by new regulations and increased regulatory scrutiny (49%) and the prevalence and high adoption of internet dependent services (40%).

These figures highlight a combination of cyber threats, regulatory issues and loss of human capital, revealing how complex the future threat landscape is perceived to be by professionals. This picture is partly mirrored by the Global Risks Report 2017 (GRR2017)[10], which lists cyber attacks as well as underemployment or unemployment as the most impactful and likely threats. Interestingly the GRR2017 sees these threats as imminent rather than emerging, showing the complexity of the threat landscape and its interpretation depending on individual roles.

Political change (38%) and the potential emergence of a global pandemic (34%) occupy the sixth and seventh positions. These two trends can be connected, for example deep political changes in countries with weak institutions might very well create the conditions for infectious diseases to spread nationally and then globally, as is the case of the Ebola crisis[11].

Looking at the UK National Risk Register 2017, global pandemics are considered to be the most imminent threat in the short term[12]. Once again, it is interesting to point out how organizations have a different view of certain threats, which tend to be regarded as more distant than they might actually be.

Increasing supply chain complexity (32%), changing consumer behaviour (30%) and climate change (30%) round up the top ten. The rising threat of climate change resonates with previous BCI research, which found how organizations consider this to be a long term concern that requires apposite planning[13].

9 For longer term it is usually meant a period of time beyond five years.
10 Global Risk Report 2017. World Economic Forum.
11 www.un.org/News/dh/infocus/HLP/2016-02-05_Final_Report_Global_Response_to_Health_Crises.pdf
12 www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf
13 Continuity Planning for Climate Change. The BCI. 2017.

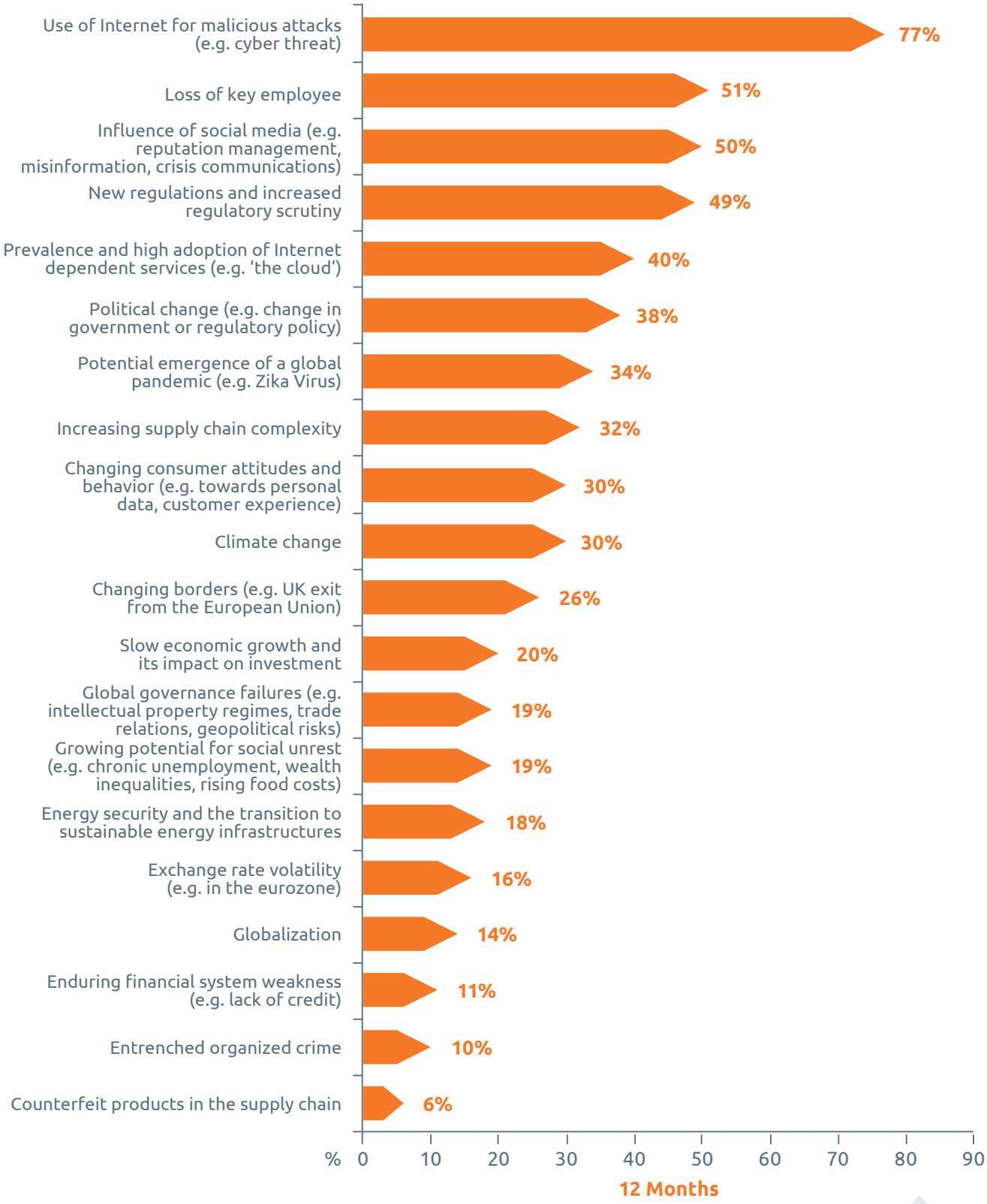


Figure 3. Which of the following trends or uncertainties are on your radar for evaluation in terms of their business continuity implications? (N=564. Answers expressed in percentage. Multiple responses allowed.)

Case study

Data breach in 2017

In 2017, a US credit reporting giant suffered a severe data breach, caused by an unpatched application that had not been updated[14].The breach compromised personal information belonging to 143 million customers, including names, social security numbers, birth dates, addresses, and license numbers. Moreover, the hack exposed roughly 209,000 US credit cards, as well as the financial history of residents in the UK and Canada[15].

According to the company's outlook released in the last quarter of 2017, profits fell below industry expectations. It was reported that the breach resulted in outlays of $60 million to $75 million. Admittedly, Equifax explained that the decline was due to delays in signing contracts with clients from both private organizations and government, as they tried to win back their trust and redeem their reputation. The company also readjusted its fourth-quarter profit forecast from an average of $1.42 to $1.32 - $1.38 per share[16].

In the US, data breaches cost organizations an average of $7 million per year due to reputational damage, legal costs, direct financial losses and recovery[17]. A recent study on the cost of data breaches worldwide revealed factors that may influence the cost of this kind of disruption, including the unexpected and unplanned loss of customers, the size of the breach, the time it takes to identify and contain it, post incident notifications, and the root cause of the breach[18].

Therefore aside from having sound cyber security arrangements, it seems costs can be mitigated during and after the incident as long as an organization and its people are well informed and trained in cyber response and disaster recovery practices. In this case, failing to update computers was a human error, despite the fact that the patch had been available for months. Hence, organizations should always pay attention to the human aspect of cyber response, as this is likely to be the cause of a breach, rather than a purely technical issue.

14 http://www.itpro.co.uk/data-leakage/29418/equifax-data-breach-hack-costs-equifax-875-million-as-income-plummets

15 O'Brien, S.A. Giant Equifax data breach: 143 million people could be affected. CNN Money. 2017 Sept 8. [cited 2018 January 4]. Available from http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

16 Reuters. Equifax Warns About Impact of Data Breach on its Business. Fortune. 2017 Nov 10 [cited 2018 January 4]. Available from http://fortune.com/2017/11/10/equifax-warns-data-breach-business/

17 Puzas, D. Data breaches cost US businesses an average of $7 million – here's the breakdown. Business Insider. 2017 Apr 27 [cited 2018 January 4]. Available from www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4

18 Ponemon Institute. 2017 Cost of Data Breach Study: Global Overview. 2017 June. [cited 2018 January 4]

Benchmarking longer term trend analysis

Year	Organizations performing trend analysis
2016	70%
2017	69%
2018	72%

Table 2. Longer term trend analysis over time.

More organizations report performing a trend analysis than last year (69% to 72%). Nevertheless, almost a quarter of organizations (23%) do not perform this at all. The increase in the percentage of organizations that practice trend analysis suggests rising awareness on its importance, with real value available when barriers are broken down and results of the analysis across different departments are shared.

43%
YES, this is conducted by a central, corporate function or department (e.g. 'strategy' or 'risk').

29%
YES, but many different departments do this according to their own needs.

23%
NO, we don't do this.

5%
I don't know.

Figure 4. Does your organization conduct longer term trend analysis as part of its horizon scanning activity? (N=579)

Nearly 7 out of 10 respondents draw upon inputs from trend analysis (68%), while those who do not have access to its results remain unchanged from last year (29%). This suggests that silos within many organizations still exist and they are a potential hindrance to organizational resilience.

44%
YES, I'm aware of the outputs and use them.

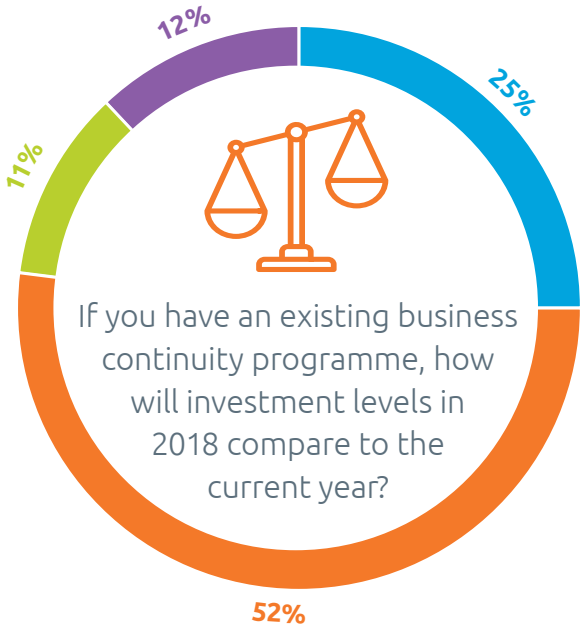
24%
YES, I help develop the analysis in the first place.

29%
NO, I do not have access to this information.

3%
NO, I don't see the value of this information.

Figure 5. As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme? (N=573)

Nearly four out of five respondents (77%) will either increase or maintain their investment in business continuity programmes in 2018. This shows improved awareness of the benefits of business continuity, regardless of the size of the organization. Indeed, small and medium enterprises (SMEs) as well as large enterprises show inclination to maintain their investments at appropriate levels, with only 6% (SMEs) and 12% (large enterprises) planning budget cuts; this is an improvement from last year's 7% and 16% respectively.



25%
Increased to meet the needs of a growing programme or new requirements.

52%
Maintained at appropriate levels for the programme scope and position in the lifecycle.

11%
Cut, limiting the scope or effectiveness of the programme.

12%
I don't know.

Figure 6. If you have an existing business continuity programme, how will investment levels in 2018 compare to the current year? (N=571)

ISO 22301 Business Continuity uptake

Year	ISO 22301 uptake
2016	51%
2017	63%
2018	70%

Table 3. ISO 22301 uptake over time.

A sound increase in the percentage of organizations that use relevant standards such as ISO 22301 was observed this year (63% to 70%). There is also a drop in the percentage of organizations not planning to use the standard at all (18% to 13%). Looking further, IT and telecommunications (86%), energy and utility (74%), and professional services (74%) are the sectors with the highest uptake of the ISO 22301 standard. It is interesting to observe that the financial and insurance sector drops out of the top three this year, however it does still continue to see adoption at over 70%.

54%
Use ISO 22301 as a framework but don't certify.

16%
Use ISO 22301 as a framework and certify against it.

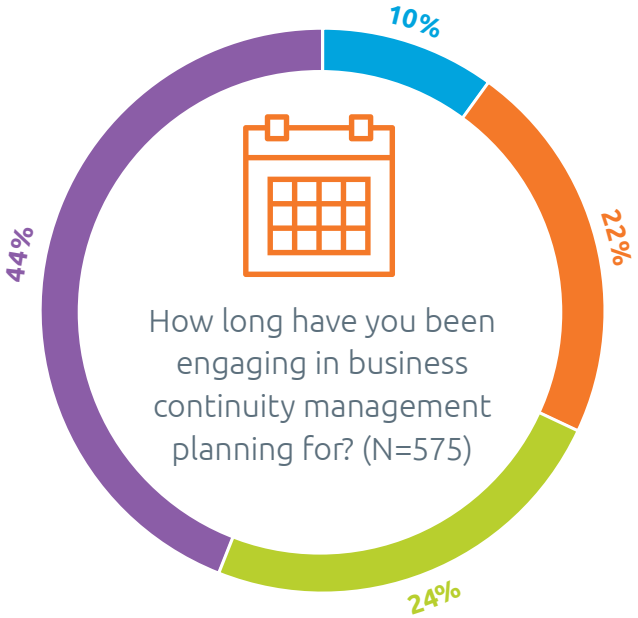
10%
Don't currently use ISO 22301 as a framework but we intend to move towards this during 2018.

13%
Don't use ISO 22301 as a framework and have no plans to move towards this during 2018.

7%
N/A

Figure 7. If you have a formal business continuity management programme in place, how does it relate to ISO 22301? (N=642)

This year the report measures the level of maturity of business continuity management within organizations. It is encouraging to see that 44% of the respondents have been adopting business continuity arrangements for longer than five years. Segmenting the data, it is interesting to observe that the longer organizations have had a business continuity programme for, the more they plan to invest in it. Among those that have had a plan for 5 years or more, 86% say they will maintain or increase their investment levels in 2018. However, out of those that have adopted business continuity processes for less than 5 years, 71% reveal they are going to do so. This could be due to the fact that in the longer term professionals begin to see a higher return on investment for their business continuity plans; which has also been widely documented in previous research[19].



10%
1 year – this is still new for the business

22%
2-3 years – this has been recently established

24%
3-5 years – this is a well-established programme

44%
5+ years – this is a mature programme

How long have you been engaging in business continuity management planning for? (N=575)

19 Business Continuity delivers return on investment. BCI. 2016.

3 Conclusions

Conclusions

1

Cyber incidents remain the biggest concern both in the long and the short term. Large-scale cyber attacks taking place in the past twelve months as well as the increasing number of internet-connected devices reaffirms the need to build cyber resilient organizations. Business continuity can play a decisive role in this, as shown by BCI research on the subject.

2

Physical security challenges of different types are also a significant threat to organizations. Extreme weather and its consequences, for instance power cuts, are particularly worrying for professionals this year. However, workplace violence incidents, such as terrorist attacks, are considered as one of the main concerns too. Workplace recovery plans can help organizations be more prepared towards physical security critical events, making staff safer and operations less vulnerable.

3

New laws and regulations are not considered as one the main challenges for organizations in the short term. However, with GDPR coming into force in May 2018 and several political changes across different geographical regions, it seems as though regulatory issues might affect organizations not before too long. Performing a sound horizon scanning analysis can definitely support professionals in understanding the threat landscape ahead.

4

The potential emergence of a global pandemic is perceived to be an issue in the longer term. However the recent Ebola crisis in West Africa and the Zika virus outbreak in South America show that this type of threat already exists and it is likely to stay as the number of diseases per decade has gone up by four times in the last sixty years[20].

5

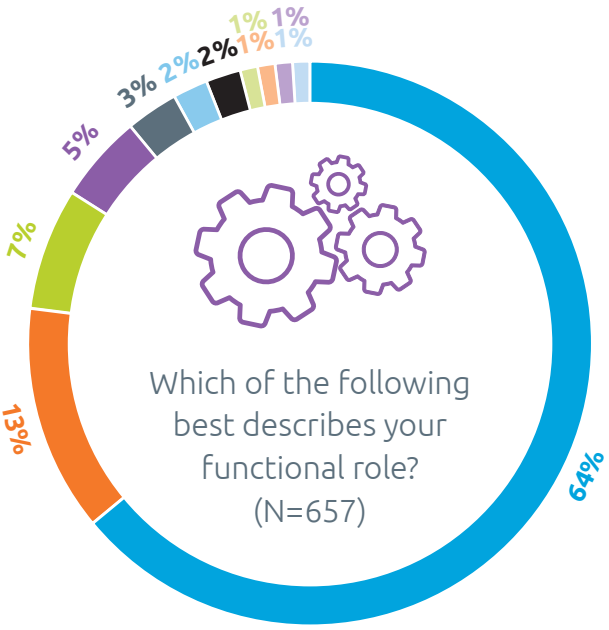
A growing number of professionals are becoming aware of benefits of business continuity. The uptake of ISO22301 is up and so is investment in BCM programmes. In addition, the longer organizations adopt and embed BCM arrangements for, the more likely they are to keep investing in them, suggesting a positive correlation with ROI.

20 time.com/4766624/next-global-security/

4 Annex

1. Demographic Information

a. Functional role of the respondents



64% Business Continuity

13% Risk Management

7% IT Disaster Recovery/ IT Service Continuity

5% Emergency Planning

3% Quality/Business Improvement

2% Security (physical/virtual)

2% Internal Audit

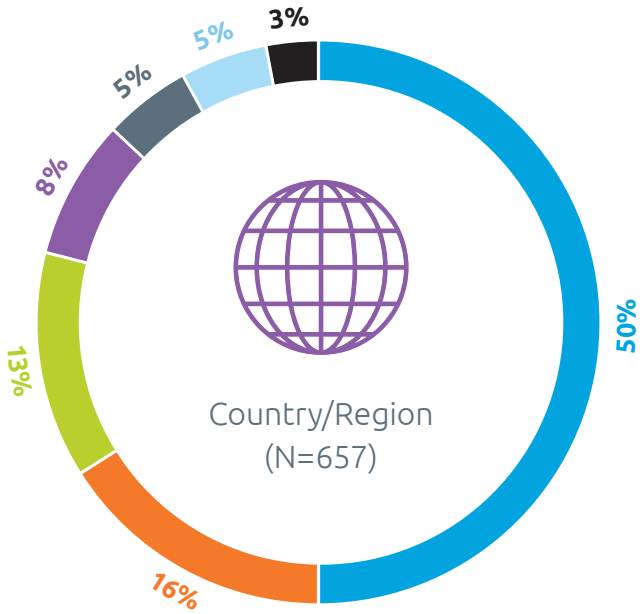
1% Health & Safety management

1% Supply chain/logistics/ procurement/purchasing

1% Line of Business/ Service Directorate

1% Supply chain/logistics/procurement/ purchasing consultant

b. Geographical base



50% Europe

16% North America

13% Asia

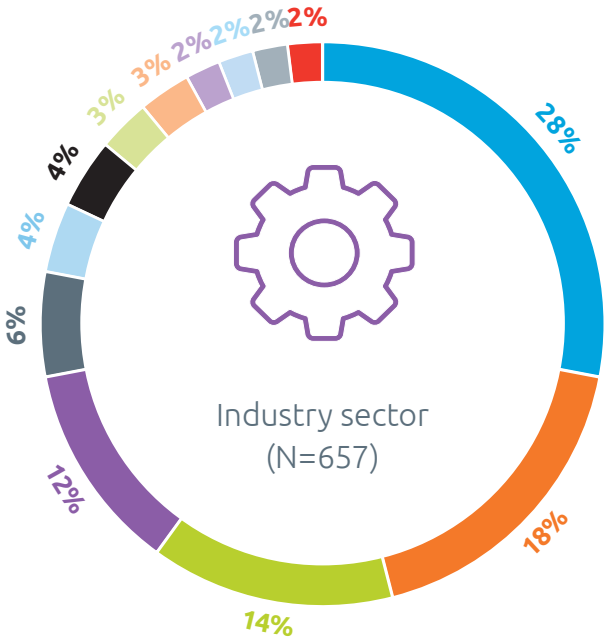
8% Australasia

5% Sub-Saharan

5% MENA

3% CALA

c. Industry sector



28% Financial & Insurance Services

18% Professional Services

14% IT & Communications

12% Public Administration & Defense (e.g. local/municipal or central government, emergency services)

6% Health & Social Care

4% Energy & Utility Services

4% Manufacturing

3% Transport & Storage

3% Retail & Wholesale

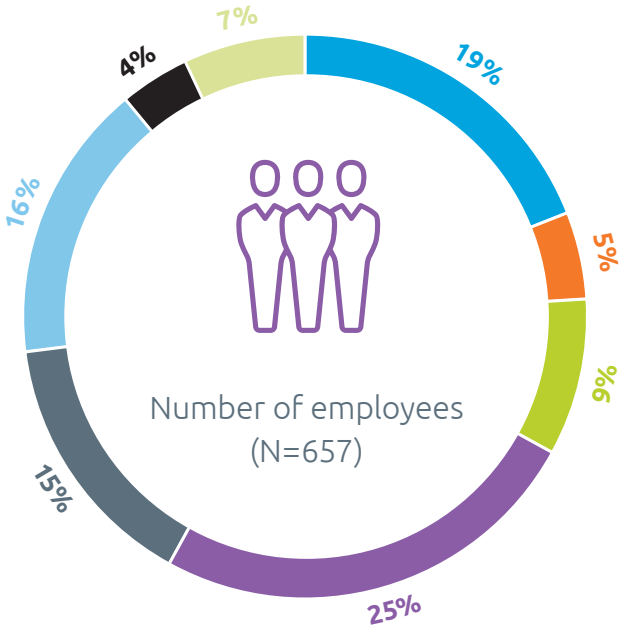
2% Education

2% Media & Entertainment

2% Support Services

2% Engineering & Construction

d. Number of employees



19% 0 - 250

5% 251 - 500

9% 501 - 1,000

25% 1,001 - 5,000

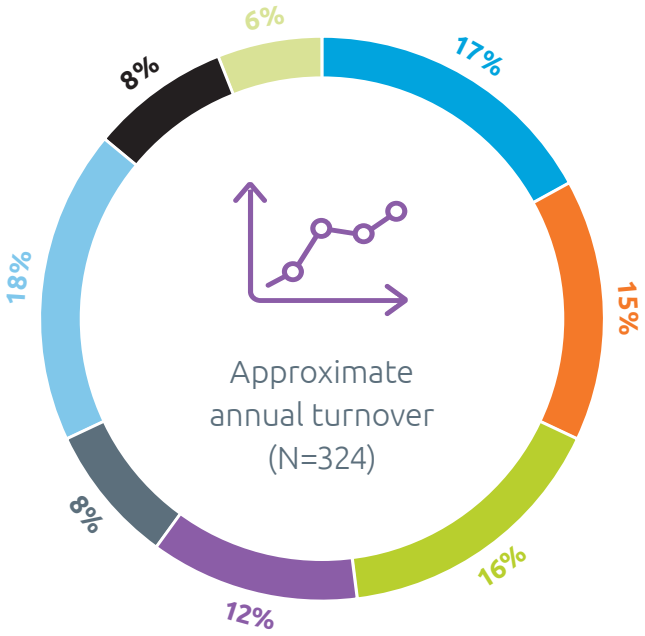
15% 5,001 - 10,000

16% 10,001 - 50,000

4% 50,001 - 100,000

7% More than 100,000

e. Approximate annual turnover



17% Less than €1 Million

15% €1 Million - €10 Million

16% €11 Million - €100 Million

12% €101 Million - €500 Million

8% €501 Million - €1 Billion

18% €1 Billion - €10 Billion

8% €11 Billion - €50 Billion

6% Greater than €50 Billion

2. Comparison by region/country

	Europe	North America	Asia	Australasia
Top three threats	**1.** Cyber attack (55%) **2.** Data breach (42%) **3.** Unplanned IT & Telecom outages (36%)	**1.** Cyber attack (53%) **2.** Data breach (44%) **3.** Unplanned IT & Telecom outages (30%)	**1.** Cyber attack (55%) **2.** Data breach (44%) **3.** Adverse weather (42%)	**1.** Cyber attack (47%) **2.** Unplanned IT & Telecom outages (43%) **3.** Data breach (40%)
Top three disruptions	**1.** Unplanned IT & Telecom outages (73%) **2.** Interruption to utility supply (45%) **3.** Cyber attack (40%)	**1.** Adverse weather (81%) **2.** Unplanned IT & Telecom outages (56%) **3.** Interruption to utility supply (44%)	**1.** Adverse weather (65%) **2.** Unplanned IT & Telecom outages (56%) **3.** Cyber attack (36%)	**1.** Unplanned IT & telecom outages (85%) **2.** Adverse weather (54%) **3.** Cyber attack (41%)
Top three trends	**1.** Use of internet for malicious attacks (80%) **2.** New regulations and increased regulatory scrutiny (52%) **3.** Influence of social media (51%)	**1.** Use of internet for malicious attacks (80%) **2.** Influence of social media (54%) **3.** Prevalence and high adoption of Internet dependent services (47%)	**1.** Use of internet for malicious attacks (65%) **2.** New regulations and increased regulatory scrutiny (52%) **3.** Loss of key employee (50%)	**1.** Use of internet for malicious attacks (78%) **2.** Loss of key employee (69%) **3.** Prevalence and high adoption of internet dependent services (56%)
Conducting Trend Analysis	77%	60%	69%	70%
Use of ISO 22301	69%	61%	76%	85%
Level of BC investment	Up 20% Down 8% Unchanged 58%	Up 33% Down 7% Unchanged 47%	Up 39% Down 10% Unchanged 43%	Up 11% Down 26% Unchanged 57%

	Middle east & North Africa	Central & Latin America	Sub-Saharan Africa	UK
Top three threats	**1.** Cyber attack (44%) **2.** Data breach (34%) **3.** Unplanned IT & Telecom outages (28%)	**1.** Cyber attack (43%) **2.** Data breach (38%) **3.** Fire (33%)	**1.** Cyber attack (37%) **2.** Unplanned IT & Telecom outages (33%) **3.** Data breach (30%)	**1.** Cyber attack (53%) **2.** Data breach (39%) **3.** Unplanned It & Telecom outages (33%)
Top three disruptions	**1.** Unplanned IT & Telecom Outages (69%) **2.** Cyber attack (46%) **3.** Interruption to utility supply (38%)	**1.** Adverse weather (53%) **2.** Interruption to utility supply (42%) **3.** Unplanned IT & telecom outages (32%)	**1.** Unplanned IT & Telecom outages (60%) **2.** Interruption to utility supply (56%) **3.** Adverse weather (32%)	**1.** Unplanned IT and telecom outages (73%) **2.** Interruption to utility supply (48%) **3.** Adverse weather (39%)
Top three trends	**1.** Use of internet for malicious attacks (66%) **2.** Influence of social media (59%) **3.** Loss of key employee (50%)	**1.** Use of internet for malicious attacks (61%) **2.** New regulations and increased regulatory scrutiny (56%) **3.** Influence of social media (56%)	**1.** Use of the internet for malicious attacks (68%) **2.** Political change (64%) **3.** Influence of social media (48%)	**1.** Use of internet for malicious attacks (80%) **2.** Influence of social media (54%) **3.** Loss of key employee (51%)
Conducting Trend Analysis	66%	65%	77%	76%
Use of ISO 22301	79%	54%	72%	70%
Level of BC investment	Up 38% Down 13% Unchanged 41%	Up 33% Down 22% Unchanged 33%	Up 21% Down 13% Unchanged 50%	Up 20% Down 7% Unchanged 58%

	US	Canada	Australia	India
Top three threats	**1.** Cyber attack (58%) **2.** Data breach (48%) **3.** Unplanned IT & Telecom outages (30%)	**1.** Cyber attack (41%) **2.** Unplanned IT & Telecom outages (32%) **3.** Data breach (32%)	**1.** Cyber attack (46%) **2.** Data breach (43%) **3.** Unplanned IT & Telecom outages (43%)	**1.** Cyber attack (63%) **2.** Adverse weather (50%) **3.** Data breach (48%)
Top three disruptions	**1.** Adverse weather (77%) **2.** Unplanned IT and telecom outages (50%) **3.** Interruption to utility supply (35%)	**1.** Adverse weather (94%) **2.** Unplanned IT and telecom outages (78%) **3.** Interruption to utility supply (72%)	**1.** Unplanned IT and telecom outages (91%) **2.** Adverse weather (57%) **3.** Cyber attack (46%)	**1.** Adverse weather (69%) **2.** Unplanned IT and telecom outages (55%) **3.** Social/civil unrest (35%)
Top three trends	**1.** Use of internet for malicious attacks (81%) **2.** Prevalence and high adoption of internet dependent services (51%) **3.** Influence of social media (51%)	**1.** Use of internet for malicious attacks (75%) **2.** Climate change (65%) **3.** Influence of social media (65%)	**1.** Use of internet for malicious attacks (76%) **2.** Loss of key employee (65%) **3.** Influence of social media (56%)	**1.** Use of internet for malicious attacks (65%) **2.** New regulations and increased regulatory scrutiny (53%) **3.** Loss of key employee (53%)
Conducting Trend Analysis	59%	64%	71%	67%
Use of ISO 22301	66%	46%	89%	81%
Level of BC investment	Up 34% Down 8% Unchanged 42%	Up 27% Down 5% Unchanged 59%	Up 14% Down 29% Unchanged 54%	Up 36% Down 4% Unchanged 51%

3. Comparison by industry sector

	Financial & Insurance	Professional services	Public administration & defence	IT & Communications
Top three threats	**1.** Cyber attack (62%) **2.** Data breach (54%) **3.** Unplanned IT and telecom outages (48%)	**1.** Cyber attack (42%) **2.** Data breach (35%) **3.** Unplanned IT and telecom outages (22%)	**1.** Cyber attack (45%) **2.** Data breach (38%) **3.** Unplanned IT and telecom outages (34%)	**1.** Cyber attack (58%) **2.** Data breach (47%) **3.** Unplanned IT and telecom outages (35%)
Top three disruptions	**1.** Unplanned IT and telecom outages (75%) **2.** Adverse weather (53%) **3.** Cyber attack (39%)	**1.** Unplanned IT and telecom outages (63%) **2.** Interruption to utility supply (44%) **3.** Adverse weather (40%)	**1.** Unplanned IT and telecom outages (78%) **2.** Adverse weather (52%) **3.** Interruption to utility supply (48%)	**1.** Unplanned IT and telecom outages (58%) **2.** Adverse weather (51%) **3.** Cyber attack (45%)
Top three trends	**1.** Use of internet for malicious attacks (78%) **2.** New regulations and regulatory scrutiny (58%) **3.** Influence of social media (55%)	**1.** Use of internet for malicious attacks (70%) **2.** Influence of social media (49%) **3.** Loss of key employee (44%)	**1.** Use of internet for malicious attacks (84%) **2.** Loss of key employee (63%) **3.** Influence of social media (49%)	**1.** Use of internet for malicious attacks (82%) **2.** New regulations and increased regulatory scrutiny (56%) **3.** Loss of key employee (50%)
Conducting Trend Analysis	81%	63%	66%	78%
Use of ISO 22301	72%	74%	68%	86%
Level of BC investment	Up 29% Down 7% Unchanged 60%	Up 24% Down 11% Unchanged 49%	Up 15% Down 25% Unchanged 44%	Up 30% Down 8% Unchanged 54%

	Health & social care	Manufacturing	Retail & Wholesale	Energy & Utility services
Top three threats	**1.** Cyber attack (62%) **2.** Unplanned telecom and IT outages (54%) **3.** Data breach (38%)	**1.** Cyber attack (41%) **2.** Supply chain disruption (41%) **3.** Product quality incident (41%)	**1.** Cyber attack (60%) **2.** Data breach (33%) **3.** Unplanned telecom and IT outages (27%)	**1.** Cyber attack (62%) **2.** Data breach (46%) **3.** Unplanned IT and telecom outages (42%)
Top three disruptions	**1.** Unplanned IT and telecom outages (70%) **2.** Cyber attack (51%) **3.** Interruption to utility supply (49%)	**1.** Supply chain disruption (52%) **2.** Unplanned IT and Adverse weather (48%) **3.** Interruption to utility supply (43%)	**1.** Unplanned It and telecom outages (87%) **2.** Adverse weather (60%) **3.** Availability of talents/ key skills (53%)	**1.** Adverse weather (56%) **2.** Unplanned IT and telecom outages (56%) **3.** Interruption to utility supply (44%)
Top three trends	**1.** Use of internet for malicious attacks (71%) **2.** Influence of social media (66%) **3.** Loss of key employee (46%)	**1.** Use of internet for malicious attacks (75%) **2.** Increasing supply chain complexity (70%) **3.** New regulations and increased regulatory scrutiny (60%)	**1.** Use of internet for malicious attacks (73%) **2.** Loss of key employee (67%) **3.** Increasing supply chain complexity (60%)	**1.** Use of internet for malicious attacks (84%) **2.** Loss of key employee (48%) **3.** Potential emergence of a global pandemic (44%)
Conducting Trend Analysis	64%	73%	86%	77%
Use of ISO 22301	68%	58%	35%	74%
Level of BC investment	Up 31% Down 6% Unchanged 42%	Up 29% Down 10% Unchanged 57%	Up 13% Down 13% Unchanged 60%	Up 19% Down 15% Unchanged 54%

4. Comparison by business size

	SMEs	Large enterprises
Top three threats	**1.** Cyber attack (35%) **2.** Data breach (29%) **3.** Unplanned IT and telecom outages (24%)	**1.** Cyber attack (57%) **2.** Data breach (45%) **3.** Unplanned IT and telecom outages (39%)
Top three disruptions	**1.** Unplanned IT and telecom outages (57%) **2.** Interruption to utility supply (41%) **3.** Adverse weather (32%)	**1.** Unplanned IT and telecom outages (69%) **2.** Adverse weather (53%) **3.** Interruption to utility supply (43%)
Top three trends	**1.** Use of internet for malicious attacks (71%) **2.** Loss of key employee (49%) **3.** Influence of social media (45%)	**1.** Use of internet for malicious attacks (78%) **2.** New regulations and increased regulatory scrutiny (52%) **3.** Influence of social media (52%)
Conducting Trend Analysis	55%	76%
Use of ISO 22301	68%	70%
Level of BC investment	Up 23% Down 6% Unchanged 55%	Up 26% Down 12% Unchanged 52%

About the Authors

Gianluca Riglietti CBCI
(BCI Research & Insight Manager)

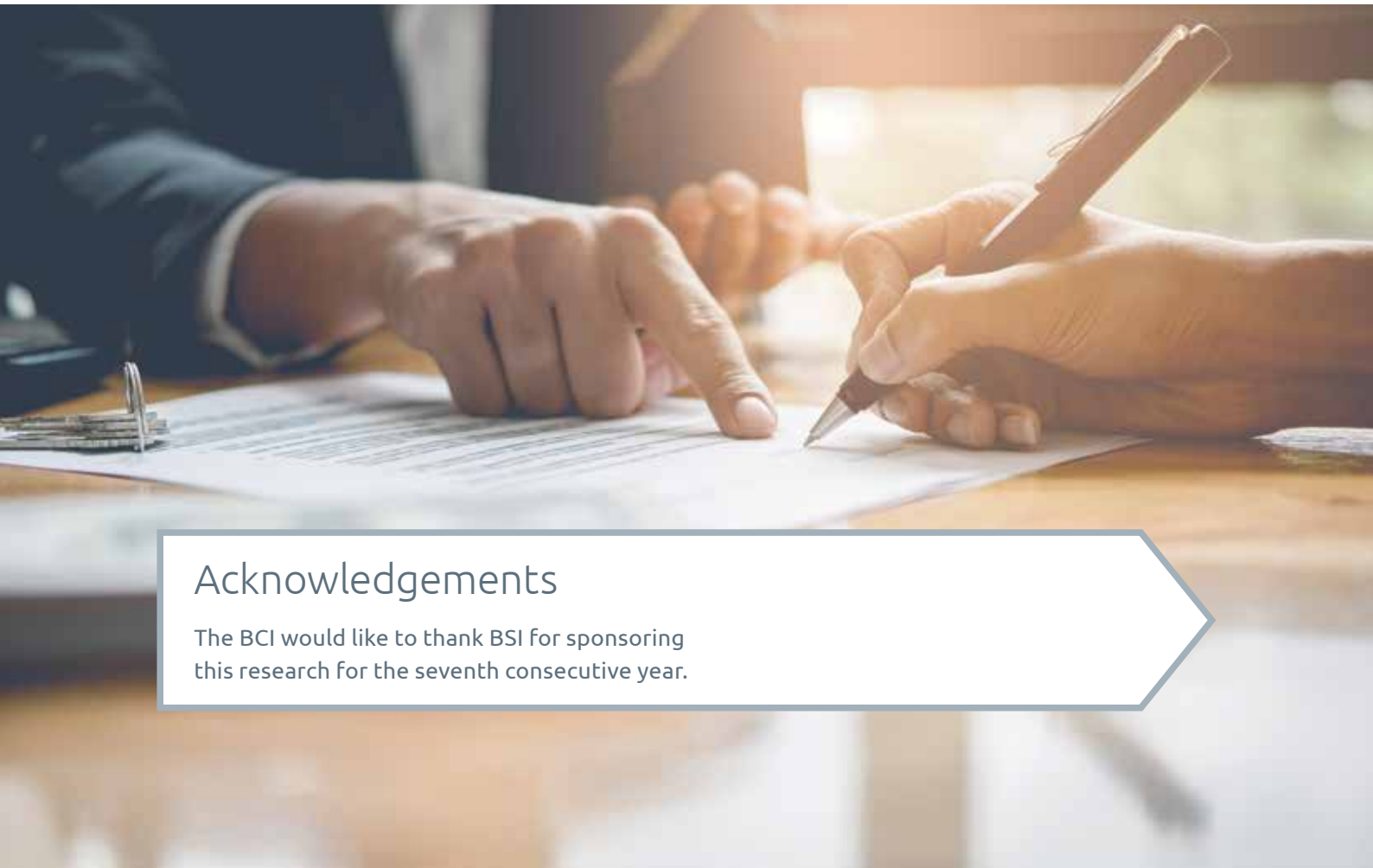
Gianluca has a Masters in Geopolitics, Territory and Security from King's College London. He has experience writing academic and industry publications, speaking at international conferences, and delivering projects for companies such as BSI, Everbridge, and Transputec. His previous professional experience includes working for the Italian Presidency of the Council of Ministers.

He can be contacted at gianluca.riglietti@thebci.org.

Lucila Aguada
(BCI Research & Insight Analyst)

Lucila is a licensed psychometrician with expertise in quantitative and qualitative research. She has a Bachelor degree and is a Masters candidate in Psychology from the University of the Philippines. She has conducted research on behalf of non-profits, pharmaceutical and healthcare clients. She is also a qualified teacher with more than seven years of experience, specialising in early childhood and special needs education.

She can be contacted at lucila.aguada@thebci.org



Acknowledgements

The BCI would like to thank BSI for sponsoring this research for the seventh consecutive year.

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.

Contact the BCI

Marianna Pallini
Communications Executive, 10-11 Southview Park
Marsack Street, Caversham, RG45AF, United Kingdom
+44 118 947 8215 | **research@thebci.org**

About BSI

BSI is the business improvement company that enables organizations to turn standards of best practice into habits of excellence.

Since it was founded in 1901 as the world's first National Standards Body, BSI has driven best practice in business around the world. Servicing 85,000 clients across 181 countries, it is a truly international organization with skills and experience across a number of sectors including automotive, aerospace, built environment, food, and healthcare.

Through its expertise in Standards and Knowledge Solutions, Assurance and Professional Services, BSI facilitates business improvement to help clients grow sustainably, manage risk and ultimately be more resilient.

To learn more, please visit: bsigroup.com

Contact BSI

Emma Joy
Global Portfolio Manager, BSI Group,
389 Chiswick High Road, London, W4 4AL, United Kingdom
+44 1908 814689 | **Emma.Joy@bsigroup.com**

Business Continuity Institute

Business Continuity Institute

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

bci@thebci.org
www.thebci.org

bsi.