Business Continuity Institute

HORIZON SCAN REPORT 2019

Correct as of January 2019

bsi.

Foreword
Business Continuity Institute

Welcome to the 2019 BCI Horizon Scan Report. The last 12 months have provided one of the most stimulating periods for Horizon Scanning that I can recall. 2018 seemed to overflow with volatile events, political and economic instability and headline grabbing disasters. Taken in combination, it could create an impression of interminable chaos. The reality is rather less dramatic, and in such times the practice of Horizon Scanning can bring beneficial focus and reason to the uncertainty.

As the BCI Good Practice Guidelines 2018 notes, **'Horizon scanning is used to monitor and identify potential threats to an organization and considers longer term change and underlying trends.'** The 2019 BCI Horizon Scan Report draws on the input of 569 global professionals to shine a light on the disruptive forces that they anticipate in 2019 and reveal how they are preparing their organizations to meet the challenge.

This is the eighth year that the BCI has published the Report, with our long-term partner, BSI. The Horizon Scan has become one of the BCI's most popular and anticipated reports and we thank BSI for their continued support.

Every Horizon Scan report produces notable results, reassuring trends and the occasional surprise. Each year, the analysis reflects the changing global environment along with the new technologies that drive economic activity. In 2019, blockchain and artificial intelligence are now identified as potential sources of disruption. What were once hard-to-predict "Black Swan' disasters have become more foreseeable 'White Swans'.

Where organizations are able to calculate the financial loss, the scan results show that reputation incidents were the second costliest form of disruption, which greatly exceed the loss from most other events, even natural disasters. As we often see, business continuity budgets continue to ebb and flow with the economic tides. 2019 shows a healthy sign of growth in budgets in 30% of organizations.

I am especially encouraged to see that nearly 4 out of 5 organizations now conduct longer term trend analysis, and that three quarters of the respondents make use of the results of their organization's trend analysis information. Access to, and use of, such intelligence is a defining attribute of resilient organizations.

For continuity and resilience practitioners the 2019 BCI Horizon Scan Report provides an invaluable information resource. The findings and analysis provide insights that can inform and confirm planning assumptions and bring fresh ideas to benefit your exercise scenarios and continuity programme.

Tim Janes
Hon FBCI
Chair of the BCI

Foreword
BSI

I'm pleased that once again BSI is supporting the BCI Horizon Scan Report 2019. Now in its eighth edition, the report, which presents findings on near and long-term business threats, has become a valuable resource to professionals working to build business continuity and Organizational Resilience. This has been demonstrated with 70% of respondents confirming that they use external reports such as the horizon scan as a risk and threat assessment tool.

Following a year of many notable disruptions – particularly with respect to adverse weather, political instability and data breaches – it's interesting to reflect on the results of this report and the financial implications of the disruptions.

IT and telecom outages, health and safety incidents and lack of talent/ key skills were rated three of the most significant disruptions in 2018, highlighting the importance of people to business success.

Health and safety incidents were not only the most prevalent, but also the costliest risk, yet in terms of impact were perceived as relatively low. However, organizations should be mindful; if the frequency increases, the impact on your bottom line can be detrimental. Organizations that do not take all threats they face seriously, and develop plans to manage them, are exposing themselves to not only reputational loss but financial costs that affect your bottom line.

It's important that organizations take a more holistic view of their business health and success, rather than just focusing on risk management. To achieve Organizational Resilience, everyone is responsible for identifying not only the big risks but also the under-rated issues that may just seem "business as usual" and can easily be missed.

This year's findings provide organizations great insight to help build a foundation so they are best placed to anticipate, prepare for and respond to change and disruption and thrive in a changing business environment.

Howard Kerr
BSI Chief Executive

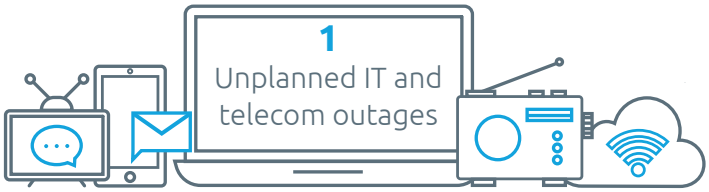
Contents

1 Executive Summary

Executive Summary

- **Technical concerns dominate:** Unplanned technical events top the list for both past disruptions and future threats: unplanned IT or telecom outages caused the most disruption in the last twelve months, whereas cyber attacks and data breaches were of most concern for the future.
- **Adverse weather is perceived as a greater threat:** A series of weather events in 2018 (such as snowstorms in Europe, wildfires in the United States and serious storms globally) means respondents view weather as a key future threat, ranked third in the list of future disruptions.
- **Political change is back in the top ten future threats:** Political change has entered the top ten list of future threats for the first time since 2015. Increasing uncertainty in Europe around Brexit, and the overall political uncertainty it brings globally are frequently cited by members as being significant challenges over the next 12 months.

Top ten disruptions - past twelve months



2
Health and safety incident

3
Lack of talent/Key skills

4
Cyber attack & data breach

5
Product quality incident/ product recall

6
Adverse weather/natural disaster (e.g. hurricane/earthquake)

7
Exchange rate volatility

8
Natural resources shortage

9
Regulatory changes

10
Higher cost of borrowing

Top ten threats - next twelve months

1
Cyber attack & data breach

2
IT and telecom outage

3
Adverse weather/natural disaster (e.g. hurricane/earthquake)

4
Critical infrastructure failure

5
Reputation incident

6
Regulatory changes

7
Lack of talent/key skills

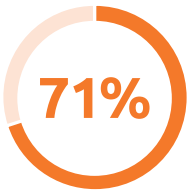
8
Supply chain disruption

9
Interruption to utility supply

10
Political change

Risk and threat assessments methods

1
Internal risk and threat assessment

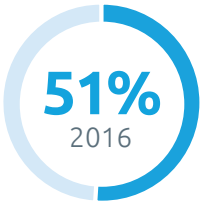


2
Risk registers

3
External reports (e.g. Horizon Scan)

ISO 22301

69% use ISO 22301 as a framework or certify against it, confirming a growing uptake over the years



Costliest disruptions (cumulative amount in USD)

1
Health and safety incidents
1.186 billion

2
Reputation incidents
1.036 billion

3
Adverse weather
500 million

4
IT and telecom outage
307 million

5
Lack of talent
254 million

6
Interruption to utility supply
244 million

7
Supply chain disruption
181 million

8
Cyber attack
144 million

9
Introduction of new technology
97 million

10
Exchange rate volatility
96 million

Organizations adopting business continuity plans for longer than one year report lower losses (6%) than the average (7%) from disruptions in the last twelve months.

Organizations planning to increase investment in the next twelve months have increased by 12% in the last five years (from 18% to 30%).

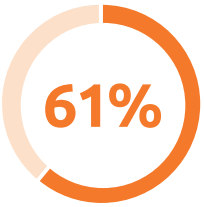
What Organizational Resilience means

Long term business survival

Business continuity

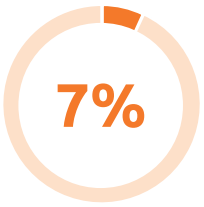
Holistic approach

Where Organizational Resilience sits



Everyone in the organization

Top management



Business continuity

2 Main report

Benchmarking business continuity

The uptake of ISO 22301 slightly decreases compared to last year (from 70% to 69%), with organizations deciding to certify against the standard also declining (from 16% to 14%). However, commitment to the standard has significantly increased through the years (Figure 2) showing it is still valuable to organizations.

55%
Use ISO 22301 as a framework but don't certify.

14%
Use ISO 22301 as a framework and certify against it.

8%
Don't currently use ISO 22301 as a framework but we intend to move towards this during 2018.

17%
Don't use ISO 22301 as a framework and have no plans to move towards this during 2019.

6%
N/A

Figure 1: If you have a formal business continuity management programme in place, how does it relate to ISO 22301?

Year	ISO22301 uptake
2016	51%
2017	63%
2018	70%
2019	69%

Figure 2. ISO22301 uptake over time.

Risk and threat assessment – past twelve months

This year the section on past disruptions to organizations includes a new analytical layer. It measures both the frequency and the impact of disruptions, for which respondents were asked to provide a score. This evolution of the methodology allows us to plot a risk score in figure 3, which better captures the extent to which a disruption affects an organization.

	Frequency*	Impact**	Risk score
IT and telecom outage	6.39	2.07	13.22
Health and safety incident	7.16	1.8	12.88
Lack of talent/key skills	5.94	2.10	12.47
Cyber attack & data breach	6.45	1.92	12.38
Product quality incident/product recall	5.62	2.01	11.29
Adverse weather/natural disaster (e.g. hurricane/earthquake)	5.03	2.20	11.06
Exchange rate volatility	5.25	2.05	10.76
Natural resources shortage	5.13	1.99	10.20
Regulatory changes	4.58	2.06	9.43
Higher cost of borrowing	4.63	2.02	9.35
Interruption to utility supply	4.85	1.92	9.31
Political violence/civil unrest	4.78	1.93	9.22
Critical infrastructure failure	3.95	2.32	9.16
Reputation incident	3.86	2.12	8.18
Supply chain disruption	4.22	1.9	8.01
Lone attacker/active shooter incident	3.55	2.25	7.98
Introduction of new technology (IoT, AI, Blockchain)	4.24	1.78	7.54
Political change	3.59	2.10	7.53
Disease outbreak	3.34	2.06	6.88

Figure 3. Risk score table. (N=411)

* Frequency of incident occurring over the past year based on group mean. Maximum score = 20

** Impact of event occurring over the past year based on group mean where 1=Minor and 4=Extreme

Non-physical disruptions

IT outages were the third most frequent interruption to business with an average impact level between moderate and major. Cyber attacks, on the other hand, were slightly more frequent but with a lower impact score, between minor and moderate. While the impact of single cyber attacks for this particular sample was not the highest, their frequency still makes the cyber threat one of the top challenges for organizations. This is consistent with similar industry reports that find cyber attacks to be one of the most recurrent threats despite not always leading to a major or extreme damage[1].

Quality assurance

Incidents involving product quality and potentially leading to a product recall were among the top disruptions in terms of frequency (5th place), with respondents reporting a moderate impact. This can be a real challenge for organizations, especially as health and safety incidents - which can be connected to the quality of the product - were the most frequent type of incident in the last 12 months. This is consistent with industry reports on health and safety incidents, for instance in the UK, where this type of hazard has increased[2]. Also, several major retailers in the UK had to withdraw different products due to health hazards over the Christmas period, ranging from clothing items to pets' food[3].

Natural disasters

Adverse weather events, such as hurricanes, snow storms and extreme heat, remain one of the main challenges to organizations, registering some of the highest impact (3rd) and frequency (8th) scores. In addition, the related issue of natural resources shortage was rated as one of the main challenges too this year, at 8th position in the risk score table. It is worth stressing that while these incidents might be referred to as black swans, according to the statistical analysis performed in this report, they have affected organizations more than five times in the last twelve months only.

Political change and new laws

Political change incidents affected organizations with relatively low frequency but with one of highest impact scores (5th), between moderate and major. In addition, a range of related disruptions such as lack of talent and key skills and exchange rate volatility are in the top ten in terms of both frequency and impact. A BCI research report on political change with a focus on Brexit reinforces this, revealing that organizations are ill prepared towards the UK exit from the European Union, especially in areas regarding employment and financial volatility[4].

1. WEF Global Risk report 2018; UK National Risk Register 2017
2. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741286/Enclosure_1_MOD_Health_and_Safety_Statistics_Annual_Report_2017-18.pdf
3. https://www.gloucestershirelive.co.uk/news/cheltenham-news/products-being-recalled-lidl-aldi-2308641
4. Brexit preparedness report

Black swans

This year's report shows that low-frequency and high-impact events, the so-called black swans, have actually affected organizations on different occasions. For instance, critical infrastructure failures have been reported as the most disruptive event and while they are not the most frequent disruption they have still affected organizations nearly 4 times on average in the past twelve months. Similarly, lone attacker incidents had the second highest impact and occurred between three and four times in the past twelve months. A similar observation is valid for extreme weather events, as previously highlighted.

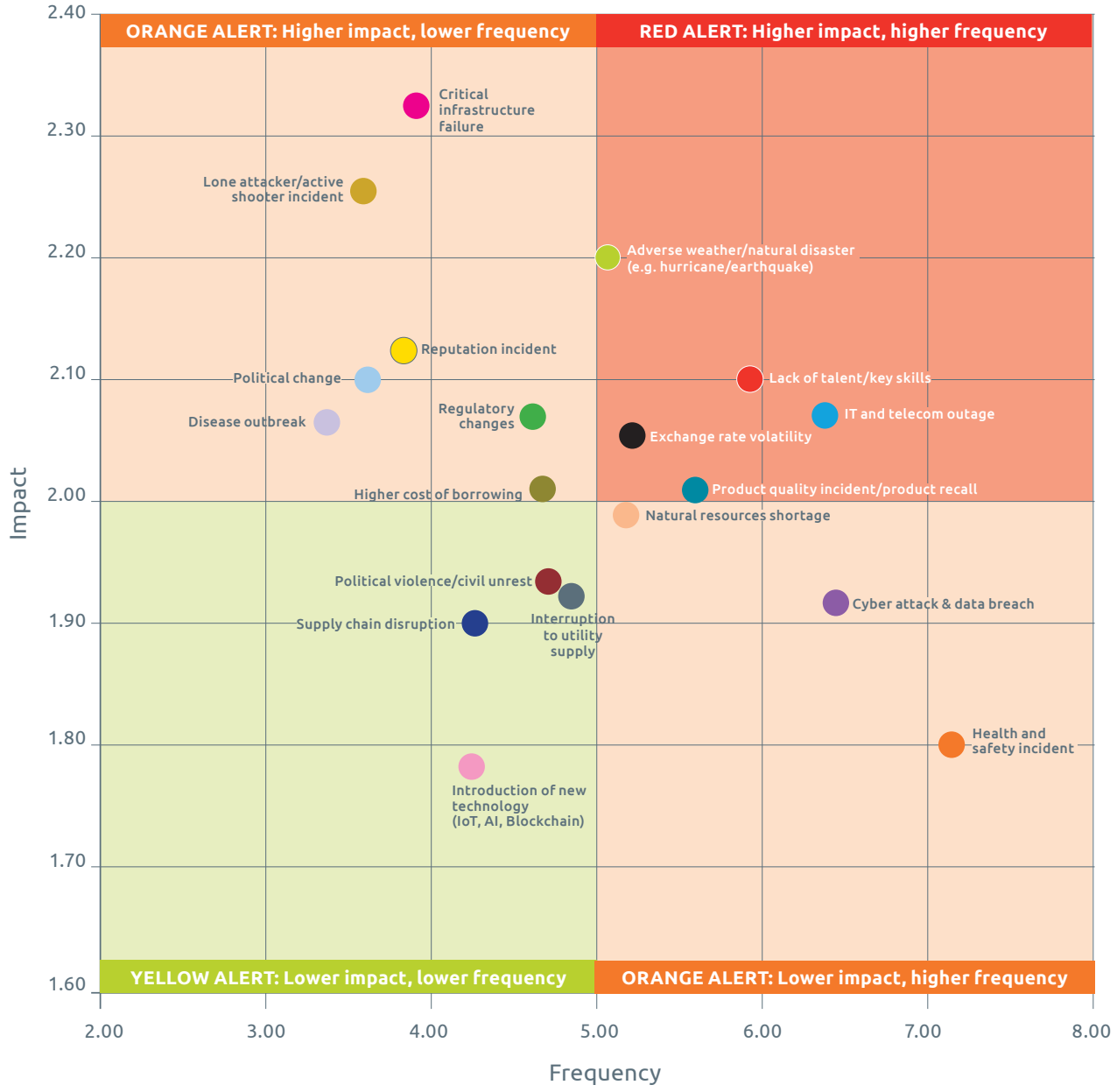


Figure 4. What was the frequency and impact of the following disruptive events? (N=411)

Risk and threat assessment: next twelve months

In this second part of the risk and threat assessment, respondents reported on future disruptions. In particular, they provided a risk score for perceived likelihood and impact of future threats occurring. The results reveal a difference between the way risks tend to be perceived in the future compared to what occurred in the past. The analysis shows how professionals' concerns divert towards high-impact threats and black swans, even though more recurring ones (e.g. health and safety incidents) can be just as damaging.

	Likelihood*	Impact**	Risk score
Cyber attack & data breach	3.25	2.17	7.05
IT and telecom outage	3.12	1.91	5.95
Adverse weather/natural disaster (e.g. hurricane/earthquake)	3.01	1.82	5.47
Critical infrastructure failure	2.48	2.19	5.43
Reputation incident	2.53	2.02	5.11
Regulatory changes	2.95	1.63	4.80
Lack of talent/key skills	2.73	1.68	4.58
Supply chain disruption	2.5	1.78	4.45
Interruption to utility supply	2.67	1.65	4.40
Political change	2.66	1.58	4.20
Introduction of new technology (Blockchain, AI, IoT)	2.63	1.57	4.12
Health and safety incident	2.69	1.53	4.11
Lone attacker/active shooter incident	1.71	2.32	3.96
Exchange rate volatility	2.31	1.57	3.62
Disease outbreak	2.01	1.7	3.41
Higher cost of borrowing	2.1	1.48	3.10
Political violence/civil unrest	1.96	1.55	3.03
Product quality incident/product recall	1.83	1.6	2.92
Natural resources shortage	1.75	1.54	2.69

Figure 5. Risk score – next twelve months (N=345)

* Likelihood of incident occurring over the next year based on group mean where 1=Remote and 5=Imminent

** Impact of event occurring over the next year based on group mean where 1=Minor and 4=Extreme

Non-physical disruptions

Cyber attacks and IT outages topped business agendas last year and continue to do so, ranking as the two highest for future concerns. It is interesting to note, however, that cyber attacks are perceived to affect organizations more in the future, as their impact score grows by 13% (from 1.92 to 2.17). In terms of likelihood, both risks are identified as being between possible and likely (3.25 likelihood score).

Political change

Political change appears as one of the top ten disruptions in the next twelve months according to its risk score (4.2) and so do other related threats such as regulatory changes (4.8), lack of talent and key skills (4.58) and supply chain disruptions (4.45). While this is somewhat consistent with the analysis of past disruptions, the financial aspect of political change seems to be neglected, as losses related to exchange rate volatility and higher cost of borrowing are ranked out of the top ten, with risk scores of 3.62 and 3.1.

Critical infrastructure failure and supply chain

Critical infrastructure failure is perceived as the fourth biggest risk in the next twelve months, with an overall impact score of 2.19, the second most impactful behind lone attacker (2.32). On a similar note, supply chain disruptions (4.45) enter the top ten future threats, ranking as number eight, being considered between possible and likely (2.5 likelihood score). Such fears might be triggered by possible complications in the flow of goods through the Strait of Dover as the UK gets closer to Brexit[5] but also by the threat of cyber attacks to critical infrastructure such as ports[6,7].

Underrated challenges

It is worth stressing that some disruptions appear to be underrated by organizations in the next twelve months. One of the clearest examples are health and safety incidents, which, despite having been the most frequent cause of disruption in the past twelve months, rank only as number twelve when looking ahead. Similarly, product quality and product recall go from being the 5th most disruptive incident in the past year to 14th in the year ahead. As highlighted above, this reveals that some of the less visible threats tend to be underrated when looking at the future. This could be because they are not perceived as malicious as a cyber attack or as extreme as adverse weather events, even though they can be highly costly and disruptive.

Black swans

Black swans are among the top concerns for organizations in the next twelve months. Risks such as critical infrastructure failure and natural disasters are among the most anticipated disruptions with high risk scores (5.47 and 5.43 respectively). The assumption that such events might occur could be a reflection on the actual frequency of such events in the past year, such as the collapse of the Morandi bridge in Italy and the California fires of 2018.

5. https://www.bbc.co.uk/news/uk-politics-46480374
6. https://www.nextgov.com/cybersecurity/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153387/
7. https://timesofsandiego.com/crime/2018/11/28/2-iranian-men-face-federal-charges-in-cyber-attack-on-port-of-san-diego/

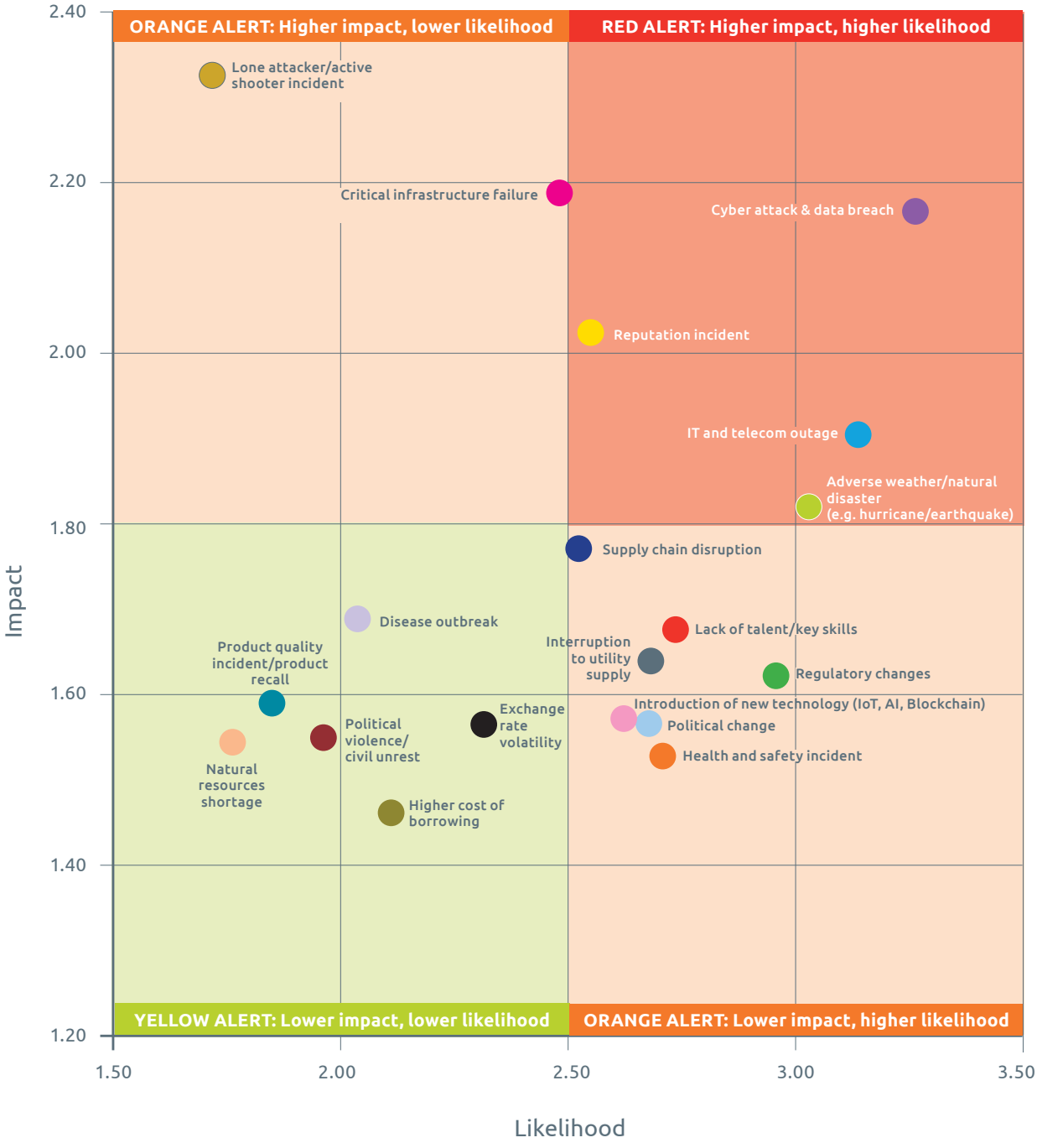


Figure 6. Risk and threat assessment – next twelve months

The majority of organizations (78%) perform trend analysis, building on last year's efforts (+6%). Furthermore, the number of professionals reporting they do not perform trend analysis at all drops by 7% this year, to 16% overall, demonstrating the growing influence of horizon scanning.

The past vs the future

Adverse weather is becoming more of a concern

Adverse weather was the fifth rated disruption in the past twelve months but has moved to third in the table for perceived future threats. An increase this year in weather related incidents such as the snowstorms affecting Europe and heatwaves in Australia has heightened concerns.

Global political uncertainty is no longer a minor issue:

Political change languished second from bottom of the risk league table for the past twelve months, but a year of political uncertainty in the US and the challenges Europe is facing around Brexit have pushed political change into the top 10 threats over the next twelve months.

Cyber attack tops the list of future challenges:

Cyber attack was the fourth greatest disruption over the past twelve months, but has now jumped to first place in the list of future threats. There were a number of high profile attacks over the past twelve months on companies which would be expected to be able to thwart attacks (such as Google and Apple) which has meant the issue is now becoming a crucial part of the board room agenda: indeed, Accenture reported spending on cyber attacks rose by 23% between 2016 and 2017 showing what a growing challenge it is.

Moving towards resilience

More than half of the respondents (51%) perceive Organizational Resilience as essential element for long-term business survival, while more than a quarter (28%) associate it with business continuity alone. Out of those who provided a different answer as the "Other" option, 70% believe that Organizational Resilience must be holistic and must include all units, such as business continuity, crisis management, incident response and disaster recovery. In line with this, almost two-thirds (61%) of the respondents are certain that everybody in an organization should be responsible for Organizational Resilience. Furthermore, over a quarter of the professionals surveyed (26%) believe Organizational Resilience should sit with top management.

What Organizational Resilience means	Where Organizational Resilience sits
Long term business survival	Everyone in the organization
Business continuity	Top management
Holistic approach	Business continuity

Figure 7. Top three terms associated with the meaning of and responsibility for Organizational Resilience.

Figure 8. What does Organizational Resilience mean to you? (N=342)

70%
All of the above

26%
Ability to prevent, respond, recover, and thrive

4%
Business continuity, crisis management, and incident response

Figure 9. What does Organizational Resilience mean to you? ("Other"; N=53)

61%
Everyone in the organization

26%
Top management

7%
Business continuity team

3%
Risk officer

2%
Others

1%
CIO

Figure 10. Who should be responsible for Organizational Resilience? (N=339)

Case study

Product quality incidents: an underrated risk

The United States Food and Drug Administration reported nearly 400 cases of product withdrawal in 2018 due to health and safety implications. For instance, a global food retailer was forced to recall over 60,000 items due to sterilisation concerns, which could have put consumer's lives in danger. Luckily, the organization acted quickly and there was no physical harm. The operation itself was quite complex, given that the incident happened during the winter holiday season, with distribution to over 26 countries, including the US. Similarly, a highly popular fast food chain had to recall one of their products due to fears there might be harmful bacteria in their salsa[1]. Health and safety hazards, unfortunately, can also be caused by malicious actors. There were several cases, in 2018, where criminals tampered with products, such as Australian strawberries and German bread, containing pins and needles, as well as contaminated sweets in Pakistan that led to more than 30 deaths[2]. As products move along an organization's supply chain, it is very difficult to identify and counter incidents of this kind, as there are multiple factors involved across different geographical regions. However, technology could provide some much-needed support. For instance, WWF have come up with a blockchain tool capable of tracking the supply chain of tuna, due to previous incidents where other types of fish were sold in cans marked as tuna. Obviously, rolling out this kind of innovation is not always a smooth process, as every link of the chain needs to embed the new technology and be aware of how to use it, which might prove to be the real challenge[3]. In addition, progress can only come by acknowledging the problem in the first place. This year's Horizon Scan shows that despite health and safety incidents being very frequent and costly, professionals tend not to see this type of incident as one of the main threats in the long term. This divergence between the perception of a risk and its actual occurrence is a threat to organizations, which might be caught unprepared when a crisis takes place.

1 https://www.fda.gov/Safety/Recalls/ArchiveRecalls/2018/default.htm?Page=1

2 https://www.dw.com/en/food-tampering-scandals-that-shocked-the-world/g-45516037

3 https://newfoodeconomy.org/blockchain-seafood-supply-chain-traseable-sea-quest-viant-wwf/

Case study

Critical infrastructure failure: black swans turning white

A black swan is an event that strikes as a surprise, with a high impact on those affected. The Black Swan Theory was coined by Nassim Nicholas Taleb in 2007 and it revolutionized the way organizations think about risk management and forecasting. One of the main messages the author tried to convey is that current risk models are not efficient enough and hard-to-predict disasters can occur due to lack of perspective[4]. Looking back at the past twelve months, it can be observed how the failure of critical infrastructure was treated as a black swan. For instance, in December 2018 a drone entered the airspace above Gatwick airport, in London, which led to all flights being grounded and delayed for several days. The situation was described by the British Transport Secretary as "unprecedented" and something that had never been seen before[5]. In this case, it is hard to disagree with Taleb when he says that black swans depend on perspective, given that previous drone activity near airports had actually already happened and had been reported; however, it was ignored. At various points over the previous two years, drones hit commercial planes in London Heathrow[6] and Quebec City[7], caused delays at London Gatwick (similarly to the December incident but on a smaller scale[8]) and terrorists in Yemen actually managed to cause an incident at Dubai airport using a drone[9]. On top of this, the Federal Aviation Administration has been warning about dangerous drone activity for years, even publishing a report with possible collision scenarios[10]. These previous warnings reveal a different picture than the one painted by the media and government statements, since this particular black swan was not an unknown or unprecedented threat. This is similar to what happened to another critical infrastructure in the UK in 2017, with the ransomware campaign that hit the UK National Health Service. The attack caused high disruption and caught many by surprise, even though similar attacks to hospitals had occurred in other countries in the previous year[11]. These instances highlight the importance of horizon scanning and preparedness. It is impossible to keep every risk under control, there will always be unknown-unknowns, but it is important to keep an open mind and try to turn as many as possible.

4 https://web.archive.org/web/20120907061933/http://www.wrap20.com/files/The_Black_Swan.pdf

5 https://www.bbc.co.uk/news/uk-england-sussex-46643173

6 https://www.bbc.co.uk/news/uk-36067591

7 https://money.cnn.com/2017/10/16/technology/drone-passenger-plane-canada/index.html

8 https://www.bbc.co.uk/news/uk-40476264

9 https://www.aljazeera.com/news/2018/07/yemen-rebels-attack-abu-dhabi-airport-drone-180726155103669.html

10 https://www.businessinsider.com/faa-report-of-drone-incidents-2016-3?r=US&IR=T

11 BCI Cyber Resilience Report 2017

3 Financial loss

The following section of the report analyses those organizations that suffered financial losses of more than 7% of their annual turnover. Through statistical analysis, a cumulative amount of financial loss per each threat was derived.

Confirming the trend spotted for past disruptions, health and safety incidents feature as the costliest event for organizations, with losses of $1.186 billion, closely followed by reputation damage at $1.036 billion. This raises further concern over the lack of attention from organizations towards risks linked to health and safety in the next twelve months. It might be also argued that the top two most costly disruptions in this chart are connected, as a health and safety incident can lead to reputation damage, receiving negative press and close scrutiny by external stakeholders[8].

Non-physical disruptions also feature prominently in the top ten, with a combined loss of more than $450 million between cyber attacks ($145 million) and IT and telecom outages ($308 million). On a similar note, the introduction of new technology, such as blockchain or artificial intelligence, amounts to $97 million. There are many reasons new technology might lead to financial losses, such as organizations losing opportunities because competitors have developed a new solution, or the actual costs to organizations of embedding new technology.

Black swans such as extreme weather events ($501 million), critical infrastructure failure ($26 million) and political change ($66 million) make this particular chart too, revealing once again that, however unlikely, highly disruptive events do happen and they carry a cost. It is worth stressing that the cumulative values shown in this section are derived from a smaller part of the sample, due to data compatibility with the analysis.

8. http://www.hse.gov.uk/business/costs-damage.htm

Financial loss

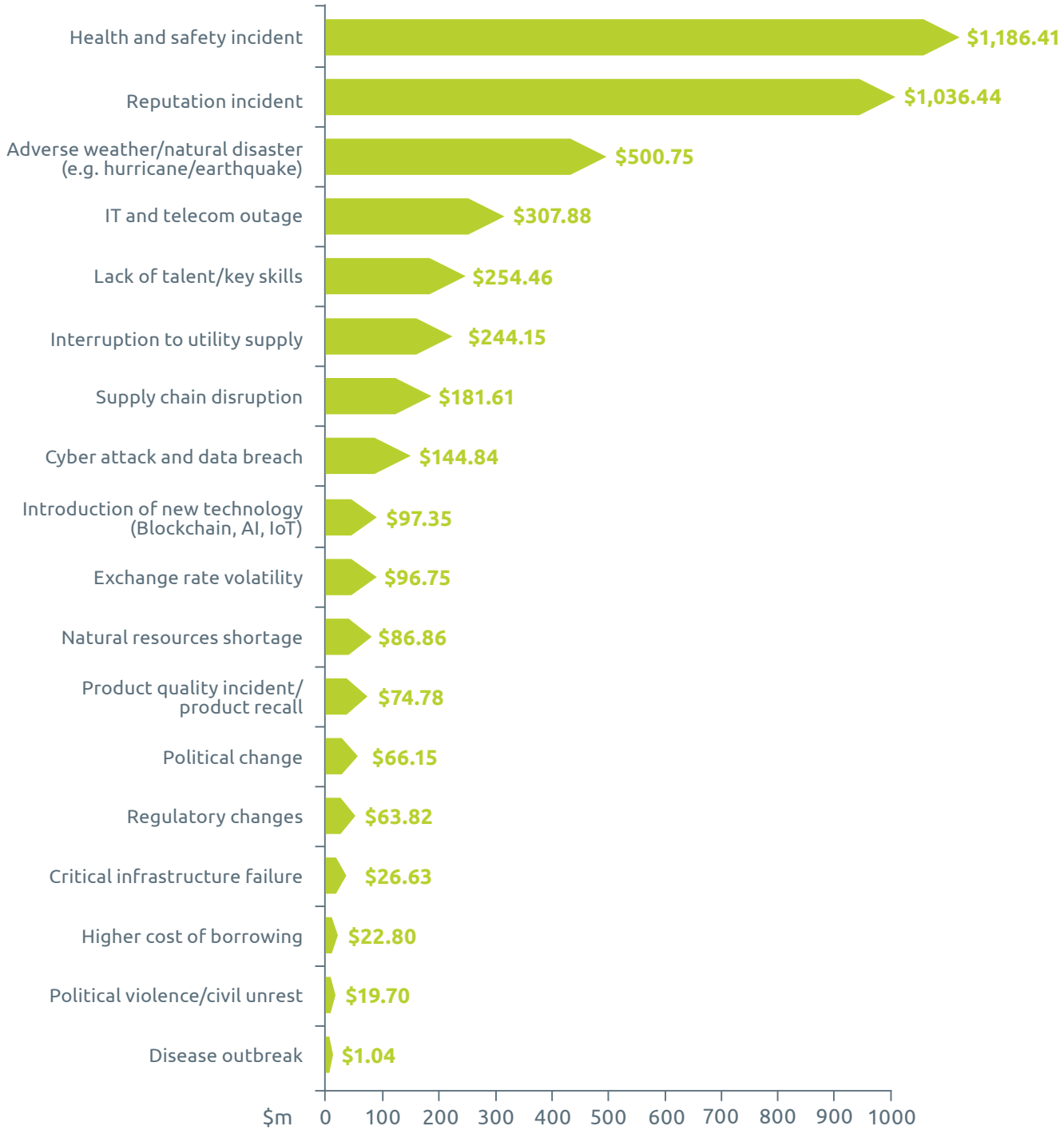


Figure 11. Disruptions resulting in the highest financial losses (more than 7% of annual turnover; N=28)

Benchmarking longer-trend analysis

Most respondents (75%) are aware and draw upon inputs from trend analysis with a 7% increase from the previous year. Moreover, those respondents who do not have access to trend analysis results or do not use its findings have also decreased by 7% (32% to 25%). This is welcome news, which could suggest that silos within organizations are breaking down, and that more practitioners can access trend analysis and other similar data. Previous BCI research reveals that building fusion centres helps reduce silos and facilitates activities such as information-sharing and joint exercises[9].

Figure 12. Does your organization conduct longer term trend analysis to better understand the threat landscape? (N=332)

Figure 13. As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme? (N=328)

9. BCI Continuity & Resilience report 2018.

Organizations' preferred way to scan for future disruptions is to conduct an internal risk and threat assessment (91%) followed by risk registers (71%) and external reports such as Horizon Scan (70%). When asked specifically about how they use this report, respondents said the Horizon Scan complements their trend analysis and it helps build informed response plans. In addition, it is included in awareness-raising initiatives to get top management buy-in. It is quite interesting to observe that technology solutions, such as social media monitoring (42%) and automated systems for cyber security (32%) are at the bottom of the table.

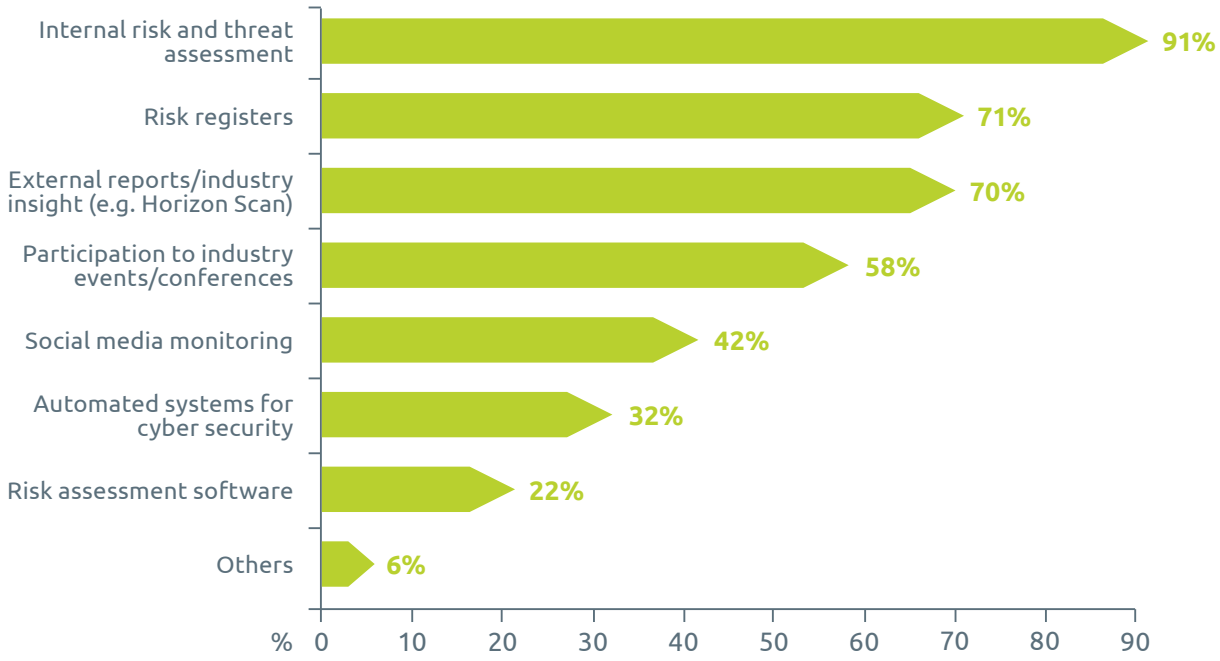
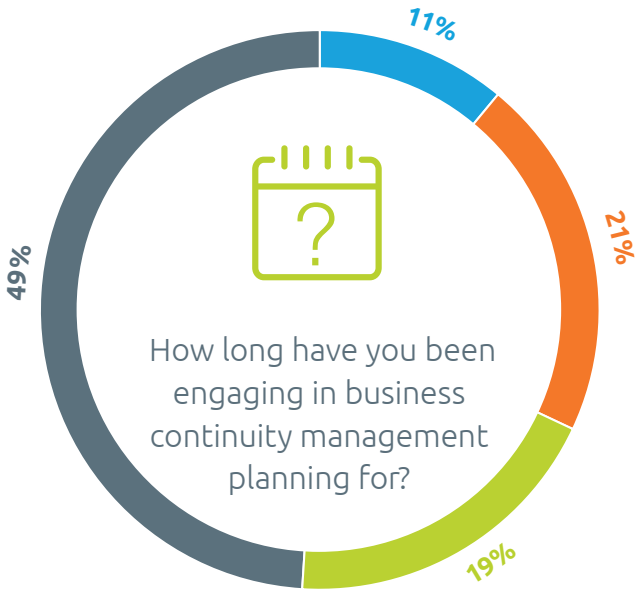


Figure 14. How do you conduct a trend analysis of the risks and threats to your organization? (N=334)

Among those organizations that are currently engaged in business continuity management planning, nearly half of them (49%) have a mature programme (five years or more), while almost one in five (19%) have been adopting such arrangements for three to five years. The number of those who have been engaging in business continuity for three years or less (33%) is rather consistent with last year's figure (32%). Further data analysis reveals how a greater longevity of business continuity arrangements is correlated with a decrease in losses due to disruptions (6%)[10], specifically to a lower level than the average (7%).

10. This refers to losses as percentage of the total annual turnover of an organization, as per question 9.



11%
1 year - this is still new for the business

21%
2-3 years - this has been recently established

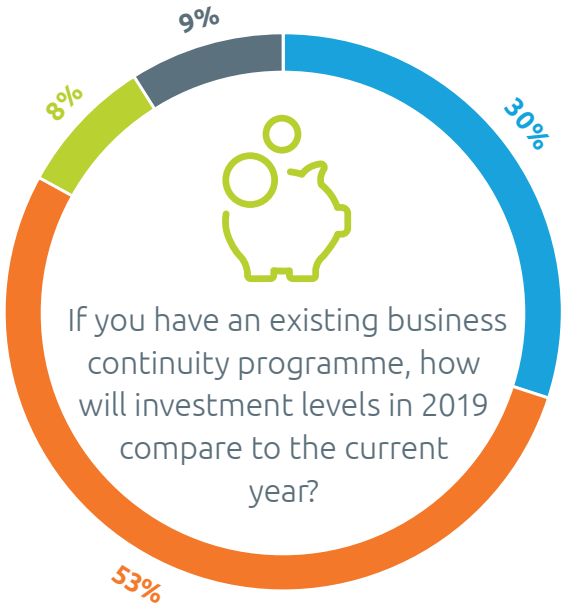
19%
3-5 years - this is a well established programme

49%
5+ years - this is a mature programme

Figure 15. How long have you been engaging in business continuity management planning for? (N=344)

Future Business Continuity investment

Professionals' appreciation of the benefits of business continuity grows by 5% (from 25% to 30%) compared to last year's results. Analysing the trend of business continuity investments, it is possible to appreciate a steady growth through the years, revealing an increased appetite and increasing resources (Table 3). This is a step in the right direction, although more improvement is needed. Indeed, previous BCI research shows how business continuity remains underbudgeted compared to other organizational functions such as risk management and information security[11].



30%
Increased to meet the needs of a growing programme or new requirements.

53%
Maintained at appropriate levels for the programme scope and position in the lifecycle.

8%
Cut, limiting the scope or effectiveness of the programme.

9%
I don't know.

Figure 16. If you have an existing business continuity programme, how will investment levels in 2019 compare to the current year? (N=329)

11. BCI Continuity & Resilience Report 2018.

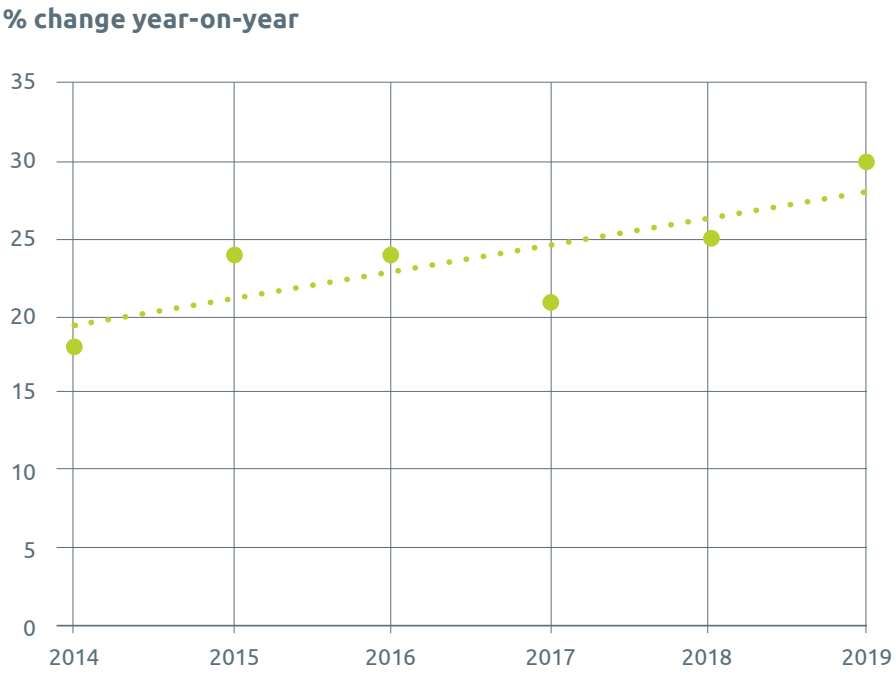
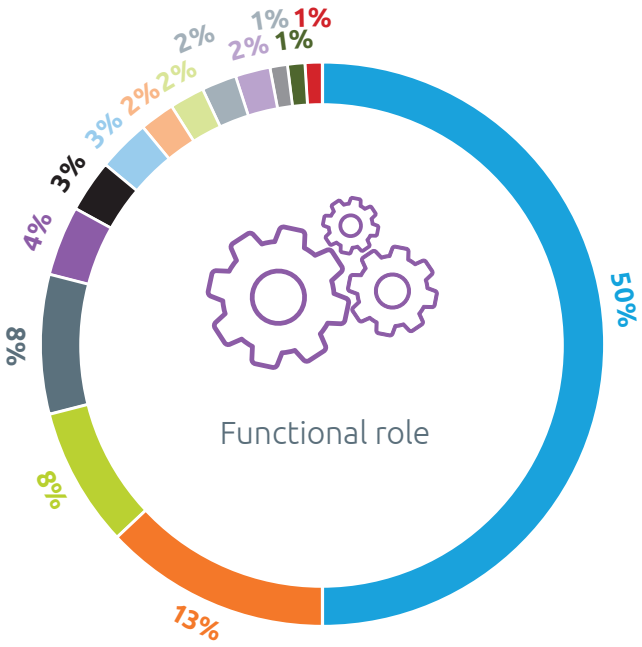


Figure 17. Percentage change year-on-year of organizations increasing business continuity investment levels

4 Annex

Demographic information



Functional role (N=569)

50% Business continuity

13% Risk management

8% Others

8% IT disaster recovery/ IT service continuity

4% Emergency planning

3% Cyber/information security

3% Crisis management

2% Quality/business Improvement

2% Health and safety management

2% Line of business/ Service Directorate

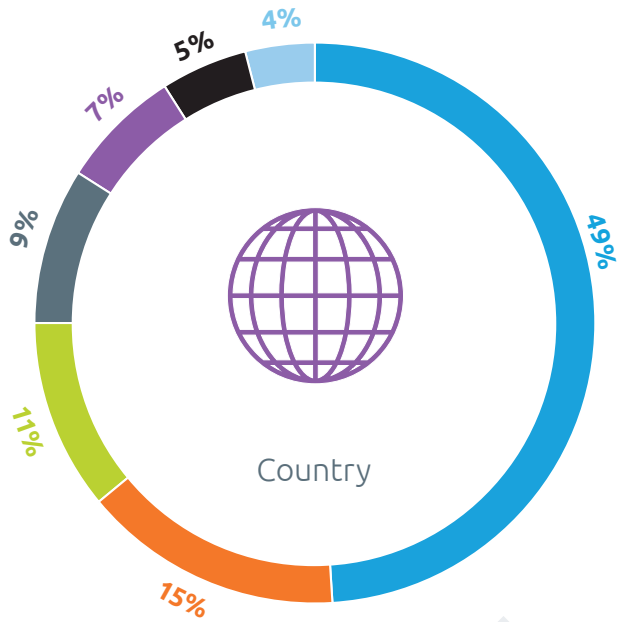
2% Internal audit

1% Security (physical)

1% Supply chain/logistics/ procurement/ purchasing

1% HR

Geographical base



Country (N=569)

49% Europe

15% North America

11% Australasia

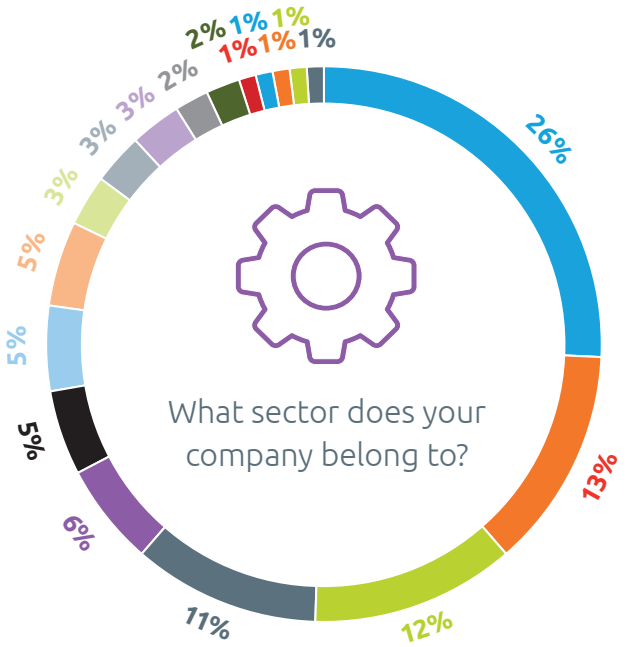
9% Asia

7% Sub Saharan Africa

5% MENA

4% CALA

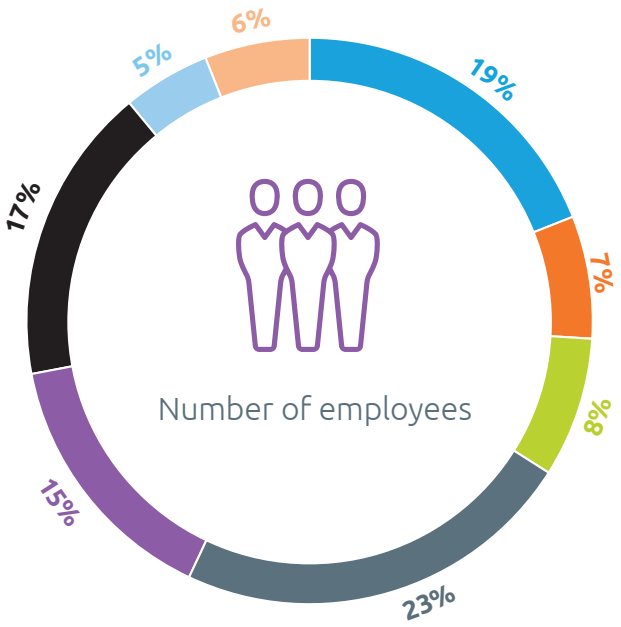
Industry sector



Q2. What sector does your company belong to? (N=569)

- **26%** Banking and finance
- **13%** Professional Services
- **12%** Public services, government and administration
- **11%** Information technology
- **6%** Energy and utilities
- **5%** Manufacturing
- **5%** Healthcare
- **5%** Others
- **3%** Education and training
- **3%** Transport and logistics
- **3%** Retail and wholesale
- **2%** Engineering and infrastructure
- **2%** Charity/Not for profit
- **1%** Emergency services
- **1%** Science and pharmaceuticals
- **1%** Law enforcement and security
- **1%** Leisure and hospitality
- **1%** Real estate and construction
- **0%** Creative industries

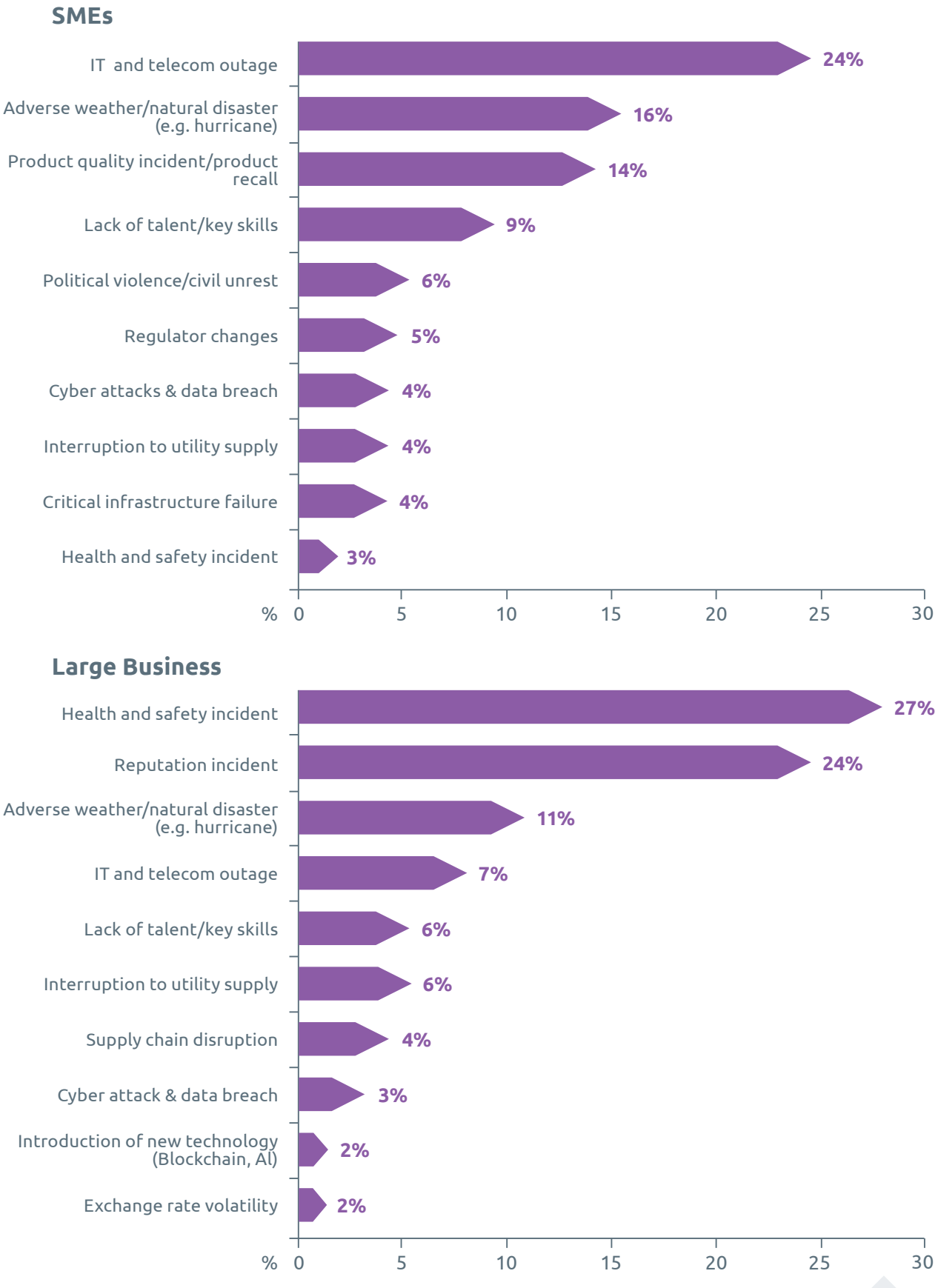
Number of employees



19% 0-250	**7%** 251-500
8% 501-1,000	**23%** 1,001-5,000
15% 5,001-10,000	**17%** 10,001-50,000
5% 50,001-100,000	**6%** More than 100,000

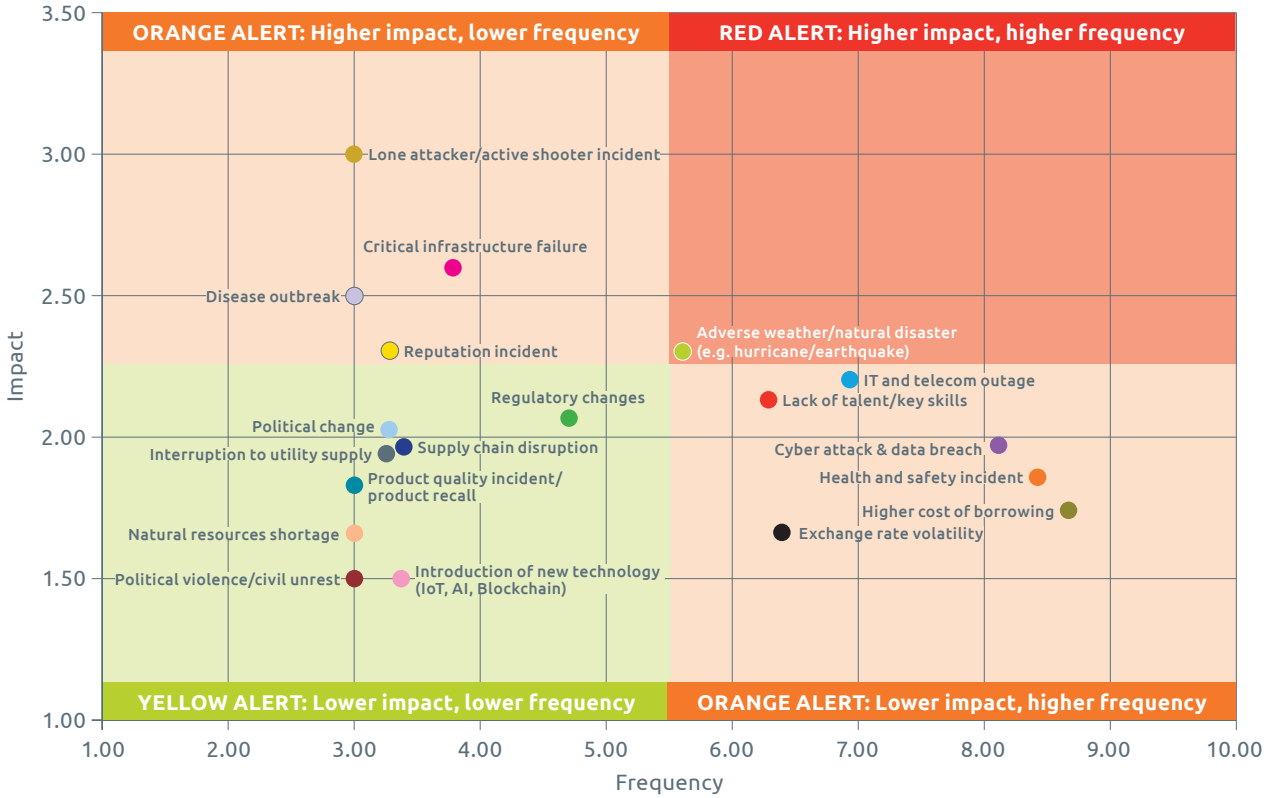
Number of employees. (N=569)

Leading financial loss drivers: SMEs and large businesses

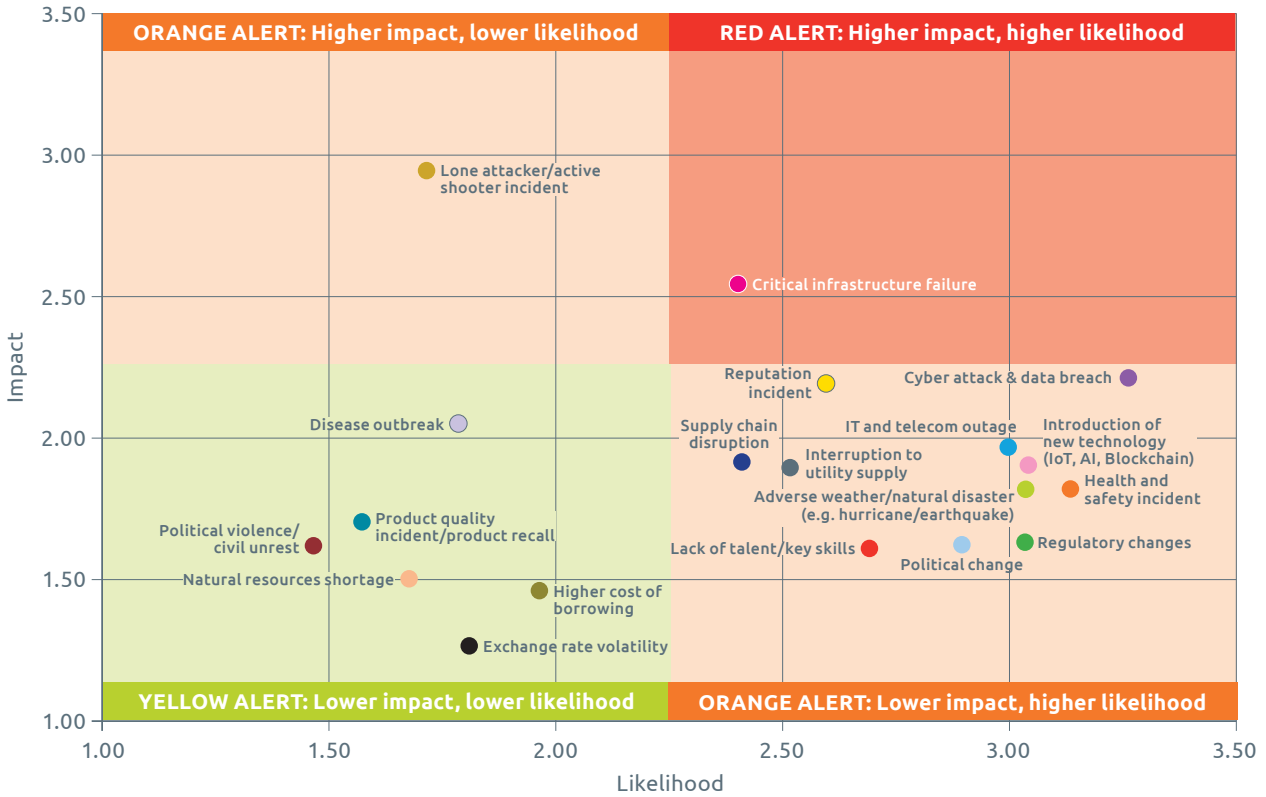


Q8 & 9. Leading Financial Loss Drivers: SME's Vs Large Business (N=27)

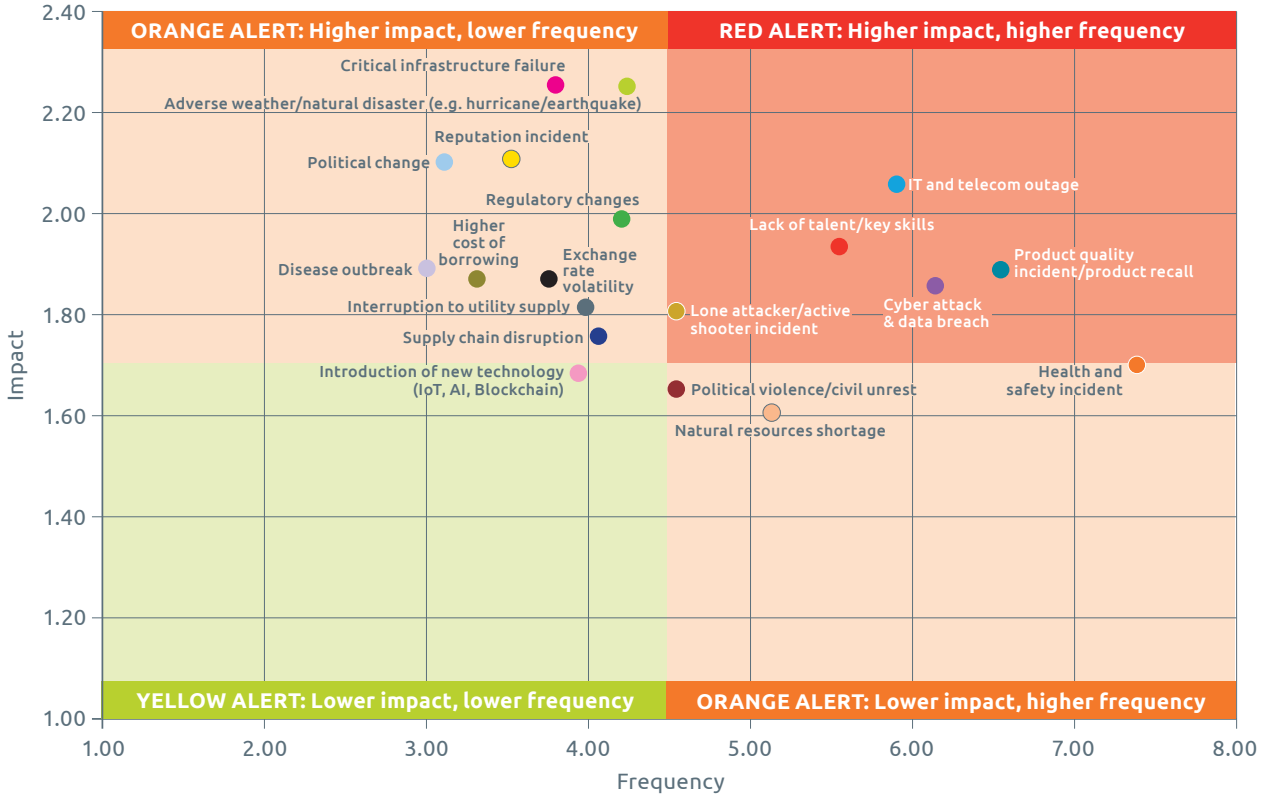
Australia: past twelve months



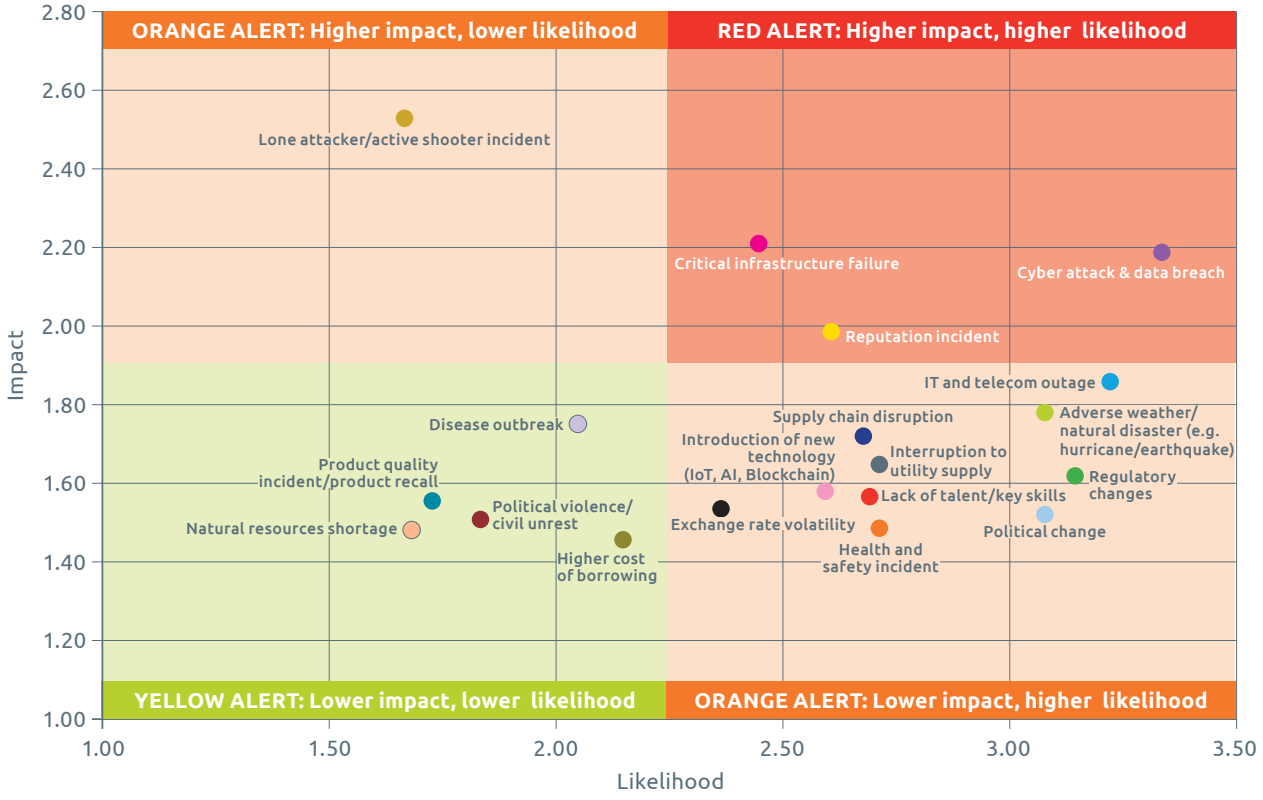
Australia: next twelve months



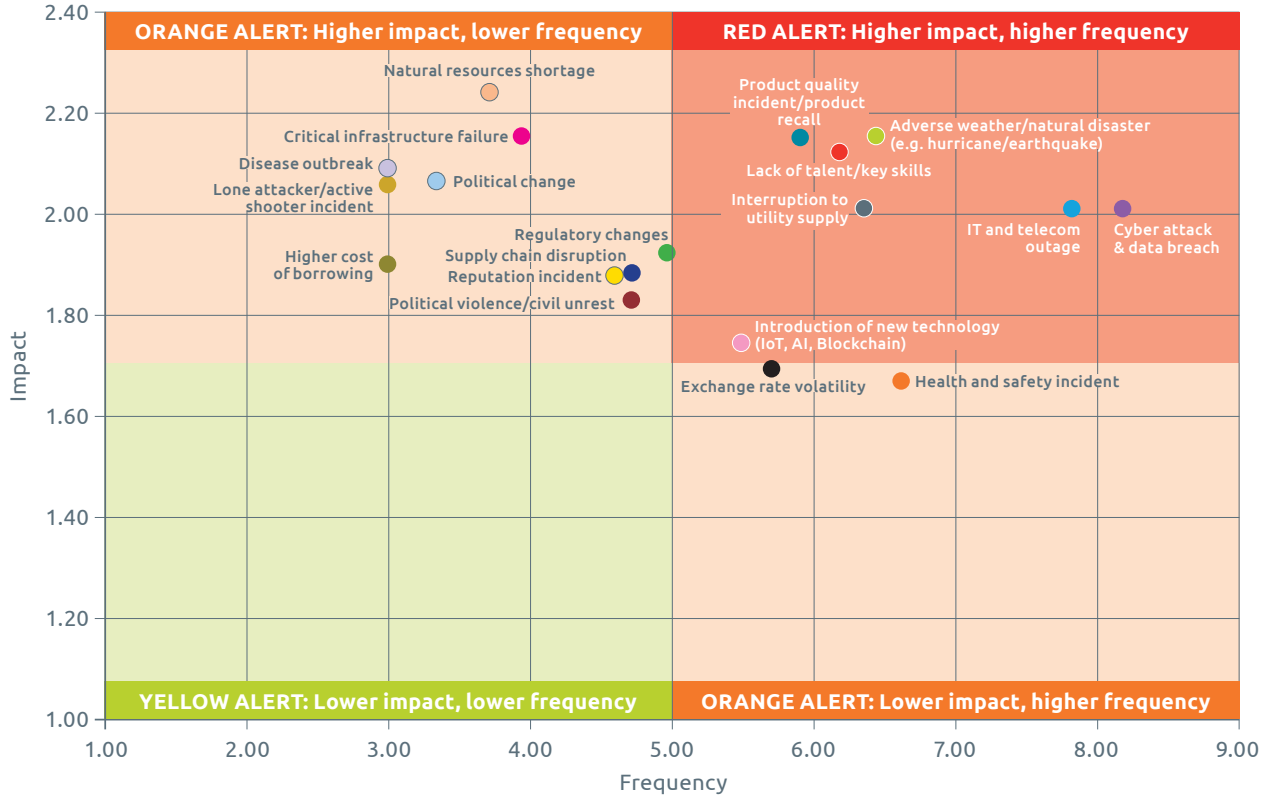
UK: past twelve months



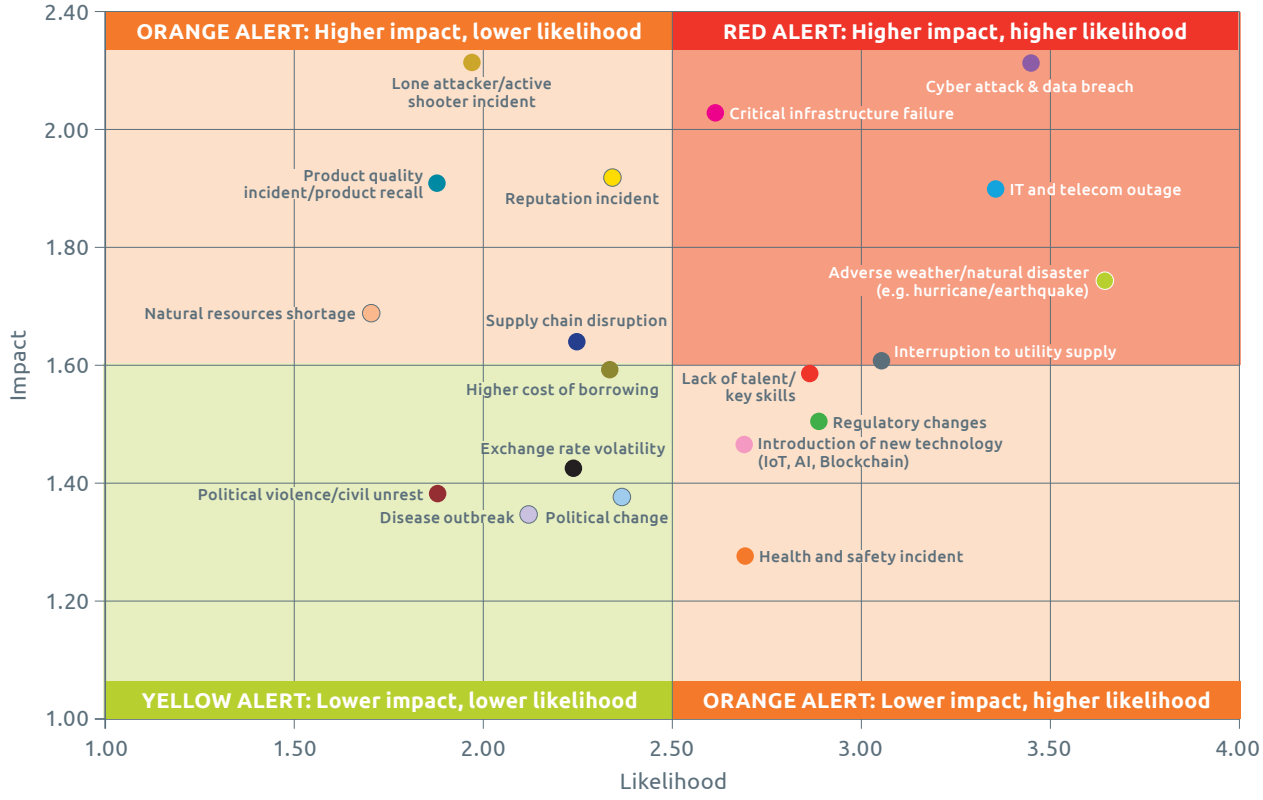
UK: next twelve months



United States: past twelve months



United States: next twelve months



About the Authors

Rachael Elliott
(Head of Thought Leadership)

Rachael has twenty years' experience leading commercial research within organizations such as HSBC, BDO LLP, Marakon Associates, CBRE and BCMS. She has particular expertise in the technology & telecoms, retail, manufacturing and real estate sectors. Her research has been used in Parliament to help develop government industrial strategy and the BDO High Street Sales Tracker, which Rachael was instrumental in developing, is still the UK's primary barometer for tracking high street sales performance. She maintains a keen interest in competitive intelligence and investigative research techniques.

She can be contacted at rachael.elliott@thebci.org.

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.

research@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

Kamal Muhammad
(BCI Research & Insight Analyst)

Kamal Muhammad is a Research Analyst at the Business Continuity Institute, he has more than five years' experience as a researcher in economics, working on economic growth and development. He previously worked as a Research Fellow/ Economist at the United Nations, where he was attached to the Macroeconomic Policy Division and was responsible for conducting policy analysis and providing technical assistance to Member States. He holds a PhD in Economics (University of Hull) and a Masters in Development Economics and Policy (University of Manchester)

He can be contacted at kamal.muhammad@thebci.org.

Acknowledgements

The BCI would like to thank BSI for sponsoring this research for the eighth 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

10-11 Southview Park,
Marsack Street, Caversham,
RG45AF, United Kingdom
+44 118 947 8215 | **bci@thebci.org**

About BSI

BSI (British Standards Institution) is the business standards company that equips organizations with the necessary solutions to turn standards of best practice into habits of excellence.

For over a century BSI has championed what good looks like and driven best practice in organizations around the world. Working with over 86,000 clients across 193 countries, it is a truly international business with skills and experience across a number of sectors including aerospace, automotive, built environment, food, and healthcare.

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

To learn more, please visit: www.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.