Find out more
www.thebci.org

Thought Leadership

BCI Horizon Scan Report 2020

An examination of the risk landscape for resilience professionals

bsi.

Leading the way to resilience

Contents

Foreword

I am delighted to introduce the 2020 BCI Horizon Scan Report. As one of the BCI's most established annual reports, the results of the Horizon Scan are always anticipated. I'd also like to thank the BSI for their continued support of the BCI Horizon Scan Report.

It is revealing each year to discover the trends in actual incidents that organizations have experienced and compare this to the future threats they anticipate. Some of these results are often as we might expect. For example, cyber-attack & data breach ranks at number one in the list of future threats for 2020. Extreme weather events are at number three, which is an understandable result given the unprecedented natural disasters that have devastated many countries in 2019.

Rather less anticipated is the position of Health Incidents at the top of the list of actual incidents that have happened over the past year. This category covers occupational disease, stress/ mental health and sickness absence. Notably, the category does not include epidemics.

At the time of writing this introduction, the spread of the coronavirus or COVID-19, the official name for the disease the virus causes, continues and is the focus of global attention. Perhaps surprisingly, with a large dose of hindsight, the relevant threat category "Non-occupational disease" is ranked at second from last in the list of Future Threats.

This result certainly reflects the timing of the Horizon Scan survey, which was conducted in the final months of 2019 when the first isolated cases had not yet been reported to the WHO.

Tim Janes
Hon FBCI, Chair of the BCI

However, this lowly position in the 2020 results illustrates how, while the world's attention is elsewhere, a different threat can suddenly erupt and cause significant disruption. Rather than one of Nassim Taleb's unforeseeable 'Black Swan' events, perhaps COVID-19 is an example of a 'Grey Swan' event. This is defined as a threat that is both predictable and extremely disruptive, but its infrequency means it is considered unlikely to occur and so it is often overlooked until its effects are all too apparent.

This reality reinforces the need for, and great value of, the Horizon Scanning activity. And not just as a once a year event, but as a regular planned activity. Many of the Horizon Scan respondents have told us they are already doing this. They have adopted a multi-faceted approach, drawing on inputs from departments across the organization as well as a range of external sources including local authorities, neighbouring businesses, peers, suppliers and publicly available reports such as the BCI Horizon Scan.

By conducting a periodic sweep of events around the world the results can be compared against the organization's response strategies and preparedness. If the scan reveals a new or unexpected threat, it's a strong incentive to take a good look at the organization's capacity to respond competently to this novel hazard.

The 2020 BCI Horizon Scan Report continues to demonstrate its value to business continuity and resilience professionals and the importance of enduring vigilance.

Foreword

We're pleased to sponsor the Horizon Scan Report once again. Now in its ninth year, it has become part of our commitment to sharing insights with organizations to enable resilience.

This year's results continue to show a disparity between what has happened around the world in the last 12 months and the threats that organizations are bracing themselves for in the year ahead. Health incidents are rated the top disruption from the previous 12 months, yet cyber-attacks and IT and telecoms outages continue to be the biggest concerns moving forward. This raises the question, are organizations complacent with operational threats? It also reinforces the importance of balancing business-as-usual risks, with those external events that sit outside of our control.

A focus on good health and wellbeing can have a hugely positive impact on employees, business culture and day-to-day delivery. Alongside increased support to help employees manage non-occupational disease, it's apparent that wellbeing strategies that look at the work causes of ill-health, such as stress, need to be a key priority for organizations when reviewing their continuity plans. This will also help attract and keep talent — another area of challenge for organizations.

The report also shows that business continuity and resilience professionals have an increased focus on internal risk and threat analysis, also apparent in our 2019 Organizational Resilience Index which highlighted that the growing pressure on businesses had caused many organizations to look inwards. This Horizon Scan benchmark complements the Index and helps organizations to make more informed business decisions.

Finally, it's promising the see the role that international standards are playing in order to support organizations to anticipate, prepare for, respond to and adapt to change — something that is more important now than ever. The increased adoption of ISO 22301 *Security and resilience: Business continuity management systems* and significant uplift in the number of organizations seeking independent certification to the standard is encouraging. The results also demonstrate that those organizations certified to the standard generally experience fewer incidents than those that are not certified. In those industries where there are fewer regulations, the value that good practice brings is clear, helping to instil confidence and support business performance. A great example of how standards can inspire trust for a more resilient world.

Howard Kerr
Chief Executive, BSI

BCI Horizon Scan Executive Summary

Executive Summary

The disruption landscape has changed over the past 12 months:
Health incidents has replaced IT and telecom outages as the leading cause of disruption for organizations over the past twelve months. There are also newer disruptions which have been noted by professionals in this year's survey: climate change, for example, has caused some organizations to halt construction projects whilst others have had to react after being targeted by climate change protestors.

Professionals' concerns for the next 12 months are still dominated by events over which they have less control:
Whilst cyber-attack and data breach is ranked as fifth in the causes of disruption for the past 12 months, it is still the leading cause of concern over the next 12 months.

Grey swans do happen:
Interestingly, non-occupational disease ranks as second last in the list of future threats: had the survey been carried out after the COVID-19 outbreak, this would undoubtedly have been higher. This shows the importance of horizon scanning and being prepared for the unexpected.

Regulatory changes cost organizations the most:
At €1.98m per incident, regulatory change costs organizations the most in terms of cost per incident with the financial services sector the one which is hit most by this category of disruption. Safety incidents are also costly, averaging €1.53m per incident.

More organizations report being certified to ISO 22301 than ever before:
20.5% of respondents report their organization is certified to ISO 22301: an increase of 6.7 percentage points on 2018. 71.0% of organizations now get certified to the standard or use it as a framework — the highest percentage ever recorded in the Horizon Scan Report.

ISO certification helps organizations to increase their resilience, but also positively affects the balance sheet:
Whilst 85.0% of respondents report ISO certification increased their organization's resilience, over a quarter (27.5%) claim it had reduced their insurance premiums.

Risk and threat assessment — past twelve months

Health incidents replace IT as the leading cause of disruption over the past twelve months

Leading causes of disruption over the past 12 months (Risk Index Rating)

Health incident: 13.9

IT and telecom outage: 13.0

Safety incident: 12.0

Lack of talent/key skills: 11.5

Cyber-attack and data breach: 11.2

Risk and threat assessment — next twelve months

Cyber-attacks remain at the top of the future threats risk index. The disconnect continues between previous incidents vs perception of future threats

Leading causes of disruption over the next 12 months (Risk Index Rating)

Cyber-attack and data breach: 6.4

IT and telecom outage: 5.4

Extreme weather events: 4.9

Critical infrastructure failure: 4.7

Lack of talent/key skills: 4.5

Consequences of disruption

The negative impact on staff wellbeing is of greater consequence than financial loss during a disruption

Leading impacts or consequences of disruption over the past 12 months

Loss of productivity: 69.3%

Negative impact on staff morale/wellbeing: 42.8%

Customer complaints received: 41.4%

Reputation damage: 39.5%

Loss of revenue: 36.3%

Financial cost of disruption

Led by responses from the financial services sector, regulatory changes cost organizations the most in terms of the average cost per disruption

The costliest disruptions to organizations (average cost per largest disruption in €m)

Regulatory change
€1.98m

Safety incident
€1.53m

Natural disaster
€1.07m

Extreme weather event
€1.00m

Cyber-attack or data breach
€0.75m

Benefits of certification

Certification helps to increase an organization's resilience, with over a quarter citing it helps to reduce insurance costs

The benefits of certification to organizations

Increases organization's resilience:
85.0%

Enables consistent BCM measurement and monitoring:
73.7%

Enables faster recovery after a disruption:
59.3%

Ensures alignment with industry peers:
54.5%

Helps to reduce insurance costs:
27.5%

Benchmarking longer term trend analysis

Most organizations carry out internal risk and threat assessments to understand factors which may impact their organization, but use of external resources is low

Methods used to conduct trend analysis of risks and threats to organizations

Internal risk and threat assessment:
86.0%

Risk registers:
62.5%

External reports/ industry insight:
58.2%

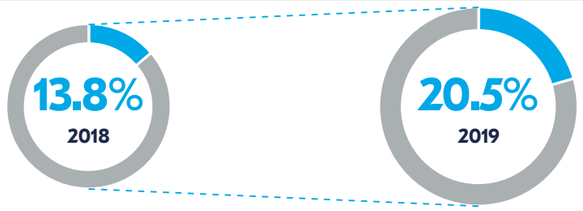
Participation in industry events/conferences:
50.1%

Social media monitoring:
32.9%

Benchmarking

Over a fifth of organizations have a business continuity management system certified to the ISO 22301 standard: a near to seven percentage point increase on 2018

Percentage of organizations certified to the ISO 22301 standard



Risk and threat assessment: past 12 months

Risk and threat assessment: past 12 months

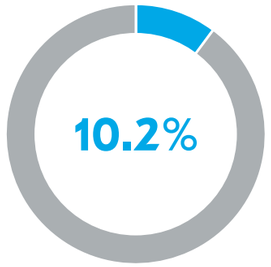
- **Health incidents replace IT and telecom outage as the leading disruption for organizations in 2019.**
- **Cyber-attacks remain a frequent challenge for organizations: whilst organizations are getting better at managing the risk of smaller attacks, large scale attacks still have the potential to cause widespread disruption to organizations.**
- **Threats such as climate change are emerging which emphasises the importance of reviewing plans in order to better understand and react to these threats accordingly.**

This year's report reveals health and safety incidents as the top cause for disruption in 2019, unseating cyber-attacks for the first time since 2014. Health incidents, which covers both pathological illness caused by working conditions and also mental illness, can have an impact on operations due to increased sickness absence and reduced productivity. In the event of a workplace-wide illness outbreak (e.g. Legionella or food poisoning), operations may close and, even if staff can work from home, employee mental wellbeing may suffer if closure is over a sustained period.

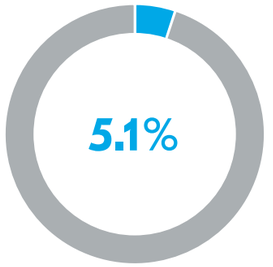
Country legislation often requires all health incidents to be recorded and monitored which could influence an organization's ability to more accurately track and monitor this kind of incident. In contrast, smaller IT or telecom outages may not be so diligently recorded.

"The disruptions we have had in the last 12 months have mainly been "business as usual" disruptions. These are generally related to changes to processes or timelines following a legislative or regulatory change, or ensuring that our staff are recognizing health and safety requirements and processes at work such as the reporting of hazards and accidents."
Resilience Analyst, Local Government, New Zealand

IT and telecom outage remains in second place this year in terms of overall impact and is still the most likely cause for multiple disruptions over the course of the year:



of respondents reported having 20 or more incidents of this kind during 2019



of organizations reported between 11-20 disruptions

Organizations cite the increasing reliance on third-party applications and services to fulfil critical business needs as a major reason for IT disruption. This demonstrates the importance of checking the business continuity arrangements of key IT/ telecommunications suppliers and ensuring recovery time objectives (RTOs) are in place for all critical products.

A 2018 report by Support Visions showed that 93% of organizations who suffered a data centre outage of 10 days or more filed for bankruptcy within a year of the event[1]. Organizations should always review the uptime statistics for their data centre provider, as well as considering a back-up provider in the case of system failure. A 99.99% uptime guarantee may appear to be sufficient, but such a guarantee actually equates to 53 minutes of downtime over the course of a year. If that happened in a busy period for an organization, the consequences could be devastating.

"As we continue to move forward with new technology solutions, we are growing our reliance more and more on third party software. When new technology such as SaaS is implemented, there are different pros and cons from business continuity risk management perspectives. If sufficient due diligence is not conducted (regularly) then the probability of an unexpected disruption would certainly increase and more when the organization is undergoing technological change."
Head of Business Continuity Management, Technology, United Kingdom

1. Support Visions 2018, Data Loss Can Cost Your Business A Huge Outage, Support Visions, viewed 7 February 2020 www.supportvisions.com/data-loss-can-cost-your-business-a-huge-outage/

Third in this year's risk index is safety incidents. 12.3% of organizations reported 11 or more safety incidents in the past year, although many of these were only minor: just 5.0% of safety incidents were classified as having a "major" or "extreme" impact and 75.0% were classified as "minor"; a higher "minor" figure than any of the other disruptions listed. This is likely to be influenced by how organizations approach incident reporting: many tend to record all safety-related incidents, regardless of the severity.

Extreme weather events are ranked in eighth place in this year's report. All countries in the world are affected by extreme weather to varying degrees: sixth in the APAC risk index, sixth in the EMEA index and third in the Americas index, illustrated in the annex section of this report. In countries that face seasonal weather disruptions such as hurricanes in North America and typhoons in the Far East, organizations typically have well-rehearsed plans for such incidences.

We once again note that cyber-attack and data breach is one of the top disruptions, placing fifth overall. Whilst the category ranks fourth in terms of frequency, the impact of cyber-attack and data breach is ranked 20th; third from bottom of the table. As noted in last year's Horizon Scan Report, whilst organizations continue to be frequently targeted by cyber criminals, they are also getting better at responding to attacks and having plans in place to recover from them. According to research by Microsoft and Marsh, 6% of organizations saw cyber risk as their primary threat in 2017. By 2019, this had increased to 22%[2]. Cyber security is now a priority on boardroom agendas and, as a result, the impact ratings suggest organizations are becoming better at managing the threat.

"There are cyber-attacks all the time, but currently not so severe that our core area of responsibility is targeted and affected."
Solutions Manager, Technology, Netherlands

"We have been subject to a number of attempted cyber breaches – viruses, phishing and one cyber-attack. The majority caused no material impact to end users, although the attack caused us to shut down servers, switch to back-ups and get all staff to reset their passwords. This resulted in around one hour lost time for access to systems for all staff and inconvenience. However, despite this there was no significant material effect for our customers as district infrastructure was not affected."
Resilience Analyst, Local Government, New Zealand

"We experience cyber attacks almost every single day mainly due to the political environment in the UK and Europe, and also in the wider world. My organization could be seen as a bit of a lever; a target - as well as Brexit in the UK. So while we believe our IT systems are not the most vulnerable, they are the most prone to attack."
Business Continuity Manager, National Government, United Kingdom

Whilst some incidences rank towards the lower end of the risk index this year, follow-up research revealed that concerns such as political change and civil unrest are causing challenges for organizations who operate in certain regions. The situation in Hong Kong, for example, has affected many global corporations which have operations within the country.

"We have an office in Hong Kong where the protests are. You wish things can get solved quickly and we can move on. But that hasn't happened, and it's been ongoing for a considerable time. We have to keep alerting staff and even on a global perspective, it does have an indirect impact on people. We have to be sensitive to the cultural and the political aspects of the issue and balance everything, by remaining entirely neutral and look out for staff wellbeing, which is the important issue."
Head of Business Continuity Management, Technology, United Kingdom

One of the issues on many resilience professionals' radars this year is climate change. Whilst climate issues have long been part of the Corporate Social Responsibility sections of annual reports, it is now having real impact on the day-to-day business operations for many organizations. The Paris Agreement, for example, is forcing many organizations to re-evaluate their emissions which can have direct impact on supply chains. Other organizations have found themselves targeted by protest groups such as Extinction Rebellion and have had to temporarily close operations. The issues being encountered are entirely new for many organizations, meaning a high proportion of organizations do not have plans in place to deal with this contemporary issue.

2. Marsh/Microsoft 2019, 2019 Global Cyber Risk Perception Survey, Marsh/Microsoft, viewed 7 February 2020 microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

"In the Netherlands, there is a governmental crisis on the environment which centres around the emission of Nitrogen which affects the natural environment and PFAS [fluorinated compounds widely used in industrial and consumer applications] in the soil. Because of this, a lot of construction projects have been halted in the Netherlands. Due to lawsuits against the government they were forced to take drastic measures which we didn't anticipate on happening. It does not affect us directly as an organization but what it does affect is construction, the construction process and construction sites. As we deliver systems and installations for buildings, if building construction stops that obviously impacts our organization directly. These are issues which have previously been unknown."
Solutions Manager, Technology, Netherlands

Since the 2019 Horizon Scan Report, we are starting to see a widening and more unpredictable risk landscape. With new threats emerging that business continuity professionals have previously seldom encountered, the importance of horizon scanning, monitoring incidents that have occurred in other organizations and updating plans accordingly is of utmost importance.

Ranking		Frequency	Impact	Risk Index
1	Health incident (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	7.5	1.9	13.9
2	IT and telecom outage	6.4	2.0	13.0
3	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	6.7	1.8	12.0
4	Lack of talent/key skills	5.6	2.1	11.5
5	Cyber-attack & data breach	6.1	1.8	11.2
6	Non-occupational disease	5.9	1.8	10.3
7	Product safety recall	5.2	2.0	10.3
8	Extreme weather events (e.g. floods, storms, freeze, etc.)	5.1	2.0	10.3
9	Interruption to utility supply	5.3	1.9	10.1
10	Exchange rate volatility	5.1	2.0	10.0
11	Natural resources shortage	4.9	2.0	9.8
12	Lone attacker/active shooter incident	4.5	2.1	9.7
13	Political violence/civil unrest	4.7	2.0	9.3
14	Introduction of new technology (IoT, AI, Big data)	4.6	2.0	9.1
15	Regulatory changes	4.3	2.1	8.8
16	Critical infrastructure failure	4.0	2.1	8.6
17	Higher cost of borrowing	4.6	1.9	8.6
18	Enforcement by regulator	3.9	2.2	8.5
19	Natural disasters (earthquakes, tsunamis, etc.)	4.0	2.1	8.4
20	Supply chain disruption	4.3	1.9	8.2
21	Energy price shock	4.3	1.9	8.2
22	Political change	3.9	2.1	7.9

Figure 1. Risk and Threat Index: Past 12 Months

Risk and Threat Assessment: Past 12 Months

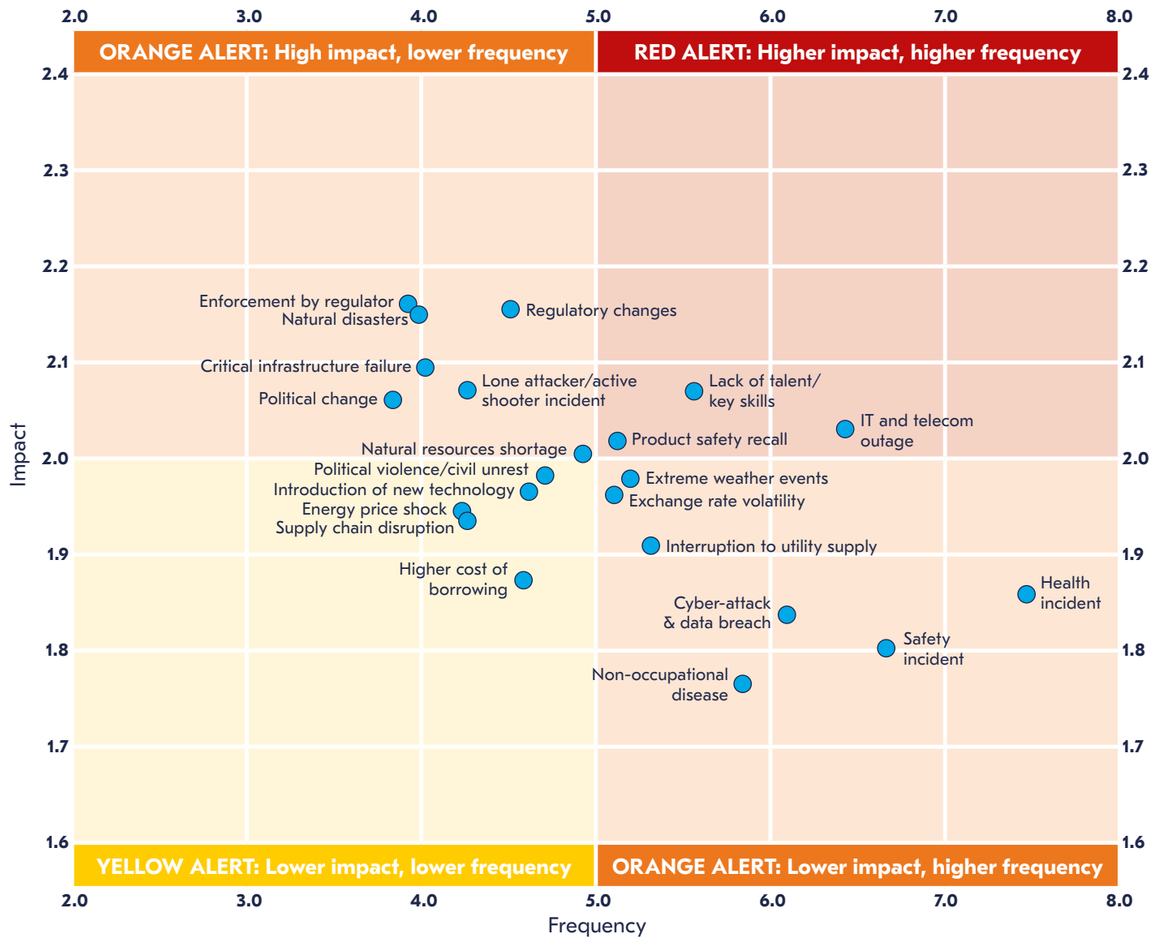


Figure 2. Risk and Threat Assessment: Past 12 Months

Risk and threat assessment: next 12 months

Risk and threat assessment: next 12 months

- **The disconnect continues between incidents that organizations have encountered over the past 12 months versus those that are top of mind for the next 12 months.**
- **Non-occupational disease ranks near the bottom of professionals' concerns over the next 12 months – but will the Coronavirus outbreak change this?**
- **Cyber-attack remains at the top of the future threats risk index.**

In this second part of the risk and threat assessment, respondents reported on future disruptions and, from this, a risk score was produced for perceived likelihood and impact of future threats occurring.

As with previous years, we once again note a disconnect between the incidences which occurred in the previous year and those which are top-of-mind concerns for the next 12 months. In the previous section, we examined how cyber-threats, whilst very frequent, are having less impact on business operations due to organizations becoming better at managing the threat. However, it again has the highest risk score in the future threats risk index. By contrast, health incidents, which topped the risk index for the previous 12 months, is in 15th position when looking forward to the next 12 months.

Professionals' concerns typically divert to those disruptions which they feel they have less control over. Extreme weather's risk score of 4.9, for example, places it in third place in the future threats risk table whereas it was ranked in eighth place in the risk table for the past 12 months. Critical infrastructure failure ranks as fourth in the list of future disruptions, but only 19th in the table for the past 12 months.

The greatest example of disconnect however is within the product safety recall category. Whilst this was seventh on the risk score table for the past 12 months, it is bottom of the table for future disruptions. The risk score is dragged down because practitioners rate the likelihood of it happening to their own company as very low. Such a disconnect could lead to organizations not being prepared to handle such a scenario both from an internal and external perspective. There have been countless examples of badly handled product recalls which have had devastating impacts on the organizations concerned:

- The car manufacturer that sent recall letters to members of the public who had already passed away due to incidents with unrecalled cars.[3]
- The fast food giant that was too quick to forgive a meatpacker who was breaking health codes.[4]
- The coffee machine manufacturer that sent a new coffee machine as recompense to a user whose home had been destroyed by fire due to a malfunctioning machine, even though a recall had been issued.[5]

Being prepared for the unexpected (which may include having pre-written communications such as press releases) can be the difference between organizational survival and liquidation.

There are, however, some disruptions which are likely to be causing additional concern over the next twelve months which may not have been considered such an issue in 2019. Political change is once again in the top 10 this year, driven by activity in certain areas of the world - from the November presidential elections in the United States to a year of uncertainty in the United Kingdom around Brexit. Political change was ranked as the fifth greatest concern for UK survey respondents.

The higher occurrences of extreme weather around the globe this year means extreme weather has held its place at third in the risk index for future threats. It was also the incident that had the highest number of respondents report that they felt the risk from extreme weather occurring over the next 12 months was "imminent". The extreme heat in Australia led to the worst bushfires in recent years, many parts of Europe encountered extreme flooding, and prolonged snowstorms in the United States saw widespread disruption throughout December, bringing the issue to top of mind for practitioners.

"Political change [is on our agenda] because of the uncertainty and because it could lead to further embargoes or trade disputes with other countries. Again, our range development and shipping areas are the US and the United Kingdom. Therefore, anything that we do, we have to comply with regulations in those countries. With the political change that's happening - you've got the US 2020 election and we just had an election here [in the UK] - things could change dramatically."
Global Business Continuity Manager, Technology, United Kingdom

"Given the recent Australian fires and climate change in general, we are expecting to see additional natural disasters over the next 10 years: floods, fires, sea level rises as well as possible tsunamis."
Resilience Analyst, Local Government, New Zealand

The risk landscape is ever evolving

Non-occupational disease is second from bottom of the table. This year's Horizon Scan survey was carried out before the outbreak of Coronavirus at the end of 2019, showing how quickly the landscape can change.

Such an issue has now become top-of-mind for organizations with many now urgently reviewing their pandemic plans for disease outbreak, particularly those organizations which have staff based in or travelling to affected regions.

Organizations are seeking insight from reports, such as the BSI Coronavirus Impact Review, to understand what the virus is, how it can spread, and the potential impacts it can have on the supply chain threat so they can respond and minimize disruption. Some larger corporations are reacting to the virus with their corporate announcements: Forbes reported 179 mentions of "coronavirus" or "outbreak" in January 2020 public transcripts[6] and some organizations, such as Starbucks, have added it as a risk to their latest quarterly filing[7]. Others are sending out press releases demonstrating their preparedness to react to disease outbreak within their organizations.

"Implementing the desired Business Continuity measures is a challenge when much of your manufacturing takes place in China and many of the components are sourced there. Ideally you would have factories in other countries and be able to redirect the production to these but that is simply not feasible. Economic aspects of running a business in a competitive market more or less dictate that you need to manufacture in countries such as China. Even if you use plants in other countries, a large proportion of the components are sourced from China so this would not effectively alleviate the disruptions that we are experiencing as a result of coronavirus. Not being able to simply switch over to an alternative manufacturing location and supply chain requires more effort on the management of the situation so as to minimise the impact.

The coronavirus presents two main challenges - the employees and the operations and we have a dedicated crisis team for each. As can be expected, our top priority is looking after our employees and ensuring their wellbeing which required close cooperation between HR, Operational Security, Health and Safety and Communications locally in China and at the global level.

The operations team focuses on managing the suppliers, production planning, distribution and managing the customers' expectations. We have defined our production priorities and are in constant contact with our key suppliers to understand what will be supplied once their production hopefully resumes on February 10 (end of extended Chinese New Year vacations). I say hopefully as there are many requirements imposed locally in order to commence production — one of these is protective masks for employees which are extremely difficult to procure. Furthermore, there are many travel restrictions imposed nationally and also locally which will impact the ability for employees to get to work and the ability to transport goods.

While we are confident that we can commence production we expect that others will struggle and that there will be many surprises and challenges to deal with in the coming weeks."
Resilience Director, Electronics Company, Netherlands

3. Janus, Andrea 2014, Family upset that GM keeps sending recall notices to their dead son, CTV News, viewed 12 February 2020, ctvnews.ca/canada/family-upset-that-gm-keeps-sending-recall-notices-to-their-dead-son-1.1896375
4. Gan, Nectar 2014, McDonald's China plans to continue using scandal-hit meat supplier OSI Group, South China Morning Post, viewed 12 February 2020, scmp.com/news/china/article/1558931/mcdonalds-plans-continue-using-scandal-hit-meat-supplier-osi-group
5. Andrews, Reed & Bailey-Shah, Shellie 2015, Keurig fire destroys apartment, company offers new coffee maker, KATU News, viewed 12 February 2020, katu.com/news/local/keurig-fire-destroys-apartment-company-offers-new-coffee-maker-11-20-2015
6. Alap Shah 2020, Coronavirus: How Companies Around The Globe Are Responding, Forbes, viewed 7 February 2020 forbes.com/sites/alapshah/2020/02/03/coronavirus-how-companies-around-the-globe-are-responding/#29f291156ab4
7. Starbucks 2020, 10Q, Starbucks, viewed 20 February 2020 s22.q4cdn.com/869488222/files/doc_financials/2020/Q1/SBUX-01292020-10-Q_As-Filed.pdf

Preparing for the unexpected is crucial. Whilst organizations trust their own processes and procedures and consider incidences such as product recalls or non-occupational disease will not happen to them, the figures show that the unexpected can happen and those organizations which have planned processes and procedures to manage such incidences are those which can thrive post-incident.

Ranking		Likelihood	Impact	Risk Index
1	Cyber-attack & data breach	3.1	2.0	6.4
2	IT and telecom outage	3.0	1.8	5.4
3	Extreme weather events (e.g. floods, storms, freeze, etc.)	2.9	1.7	4.9
4	Critical infrastructure failure	2.3	2.0	4.7
5	Lack of talent/key skills	2.6	1.7	4.5
6	Regulatory changes	2.6	1.7	4.4
7	Natural disasters (earthquakes, tsunamis, etc.)	2.0	2.1	4.2
8	Interruption to utility supply	2.6	1.6	4.0
9	Introduction of new technology (IoT, AI, Big data)	2.6	1.5	4.0
10	Political change	2.4	1.6	3.8
11	Supply chain disruption	2.2	1.7	3.8
12	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	2.5	1.5	3.8
13	Lone attacker/active shooter incident	1.8	2.1	3.6
14	Enforcement by regulator	2.1	1.7	3.6
15	Health incident (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	2.4	1.5	3.5
16	Political violence/civil unrest	2.1	1.6	3.2
17	Exchange rate volatility	2.1	1.4	3.0
18	Higher cost of borrowing	1.9	1.4	2.7
19	Energy price shock	1.9	1.4	2.7
20	Natural resources shortage	1.7	1.5	2.5
21	Non-occupational disease	1.8	1.3	2.4
22	Product safety recall	1.5	1.4	2.1

Figure 3. Risk and Threat Index: Next 12 Months

Risk and Threat Assessment: Next 12 Months

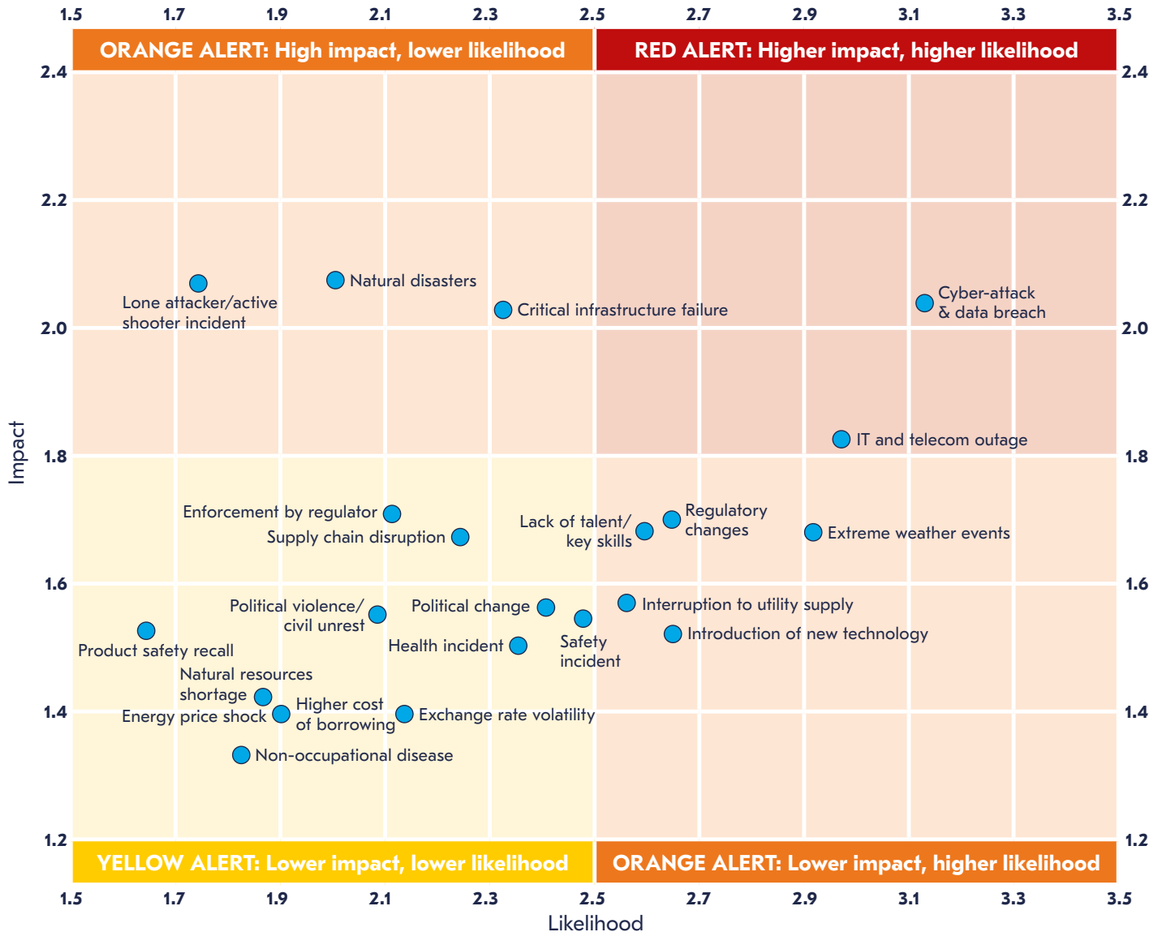


Figure 4. Risk and Threat Assessment: Next 12 Months

Consequences of disruptions

Consequences of disruptions

- **Loss of productivity is the most frequently cited consequence of disruption with 69.3% of organizations reporting this.**
- **The negative impact on staff wellbeing is in second place, surprisingly ahead of financial impact.**
- **Loss of revenue as a consequence of disruption was only cited by just over a third (36.3%) of organizations.**

This year, a new section has been introduced to look at the impacts and consequences of the disruptions organizations have faced over the past year. Whilst loss of productivity was, rather unsurprisingly, the top-rated response at 69.3%, the second response, negative impact on staff morale/wellbeing, might come as a surprise to many given it is positioned ahead of customer complaints, reputation damage and loss of revenue. Christine Probett, a management and human resource professor at San Diego State University said in an article published on NBC News that "many companies focus externally only" during crisis situations and "if there is no internal communication, employees expect the worst and productivity drops significantly when employees speculate on what might happen."[8] The results suggest organizations are recognizing the impact of employee morale/wellbeing on productivity. The BCI's 2020 Emergency Communications Report highlighted how certain tools can be used during a crisis to improve morale e.g. using WhatsApp groups as a casual communication tool amongst staff during an emergency ensures staff can communicate with peers and reduce feelings of isolation[9].

Loss of revenue was only cited by just over a third of respondents (36.3%) and delayed cash flows by just 12.8% of respondents suggesting that many organizations can manage disruptions before they take a direct hit on revenues. For smaller disruptions, this is understandable but for larger disruptions (such as the loss of a production site), the most diligent organizations will be able to move production to back-up sites to ensure continuity of service.

8. Tahmincioglu, Eve 2010, Surviving Your Company's Mistakes, NBC News, Accessed 7 February 2020 nbcnews.com/id/37108260/ns/business-careers/t/surviving-your-companys-mistakes/
9. The BCI 2020, Emergency Communications Report 2019, The BCI, Accessed 7 February 2020 thebci.org/resource/bci-emergency-communications-report-2020.html

Which of the following impacts or consequences arose from the disruptions experienced in the last 12 months?

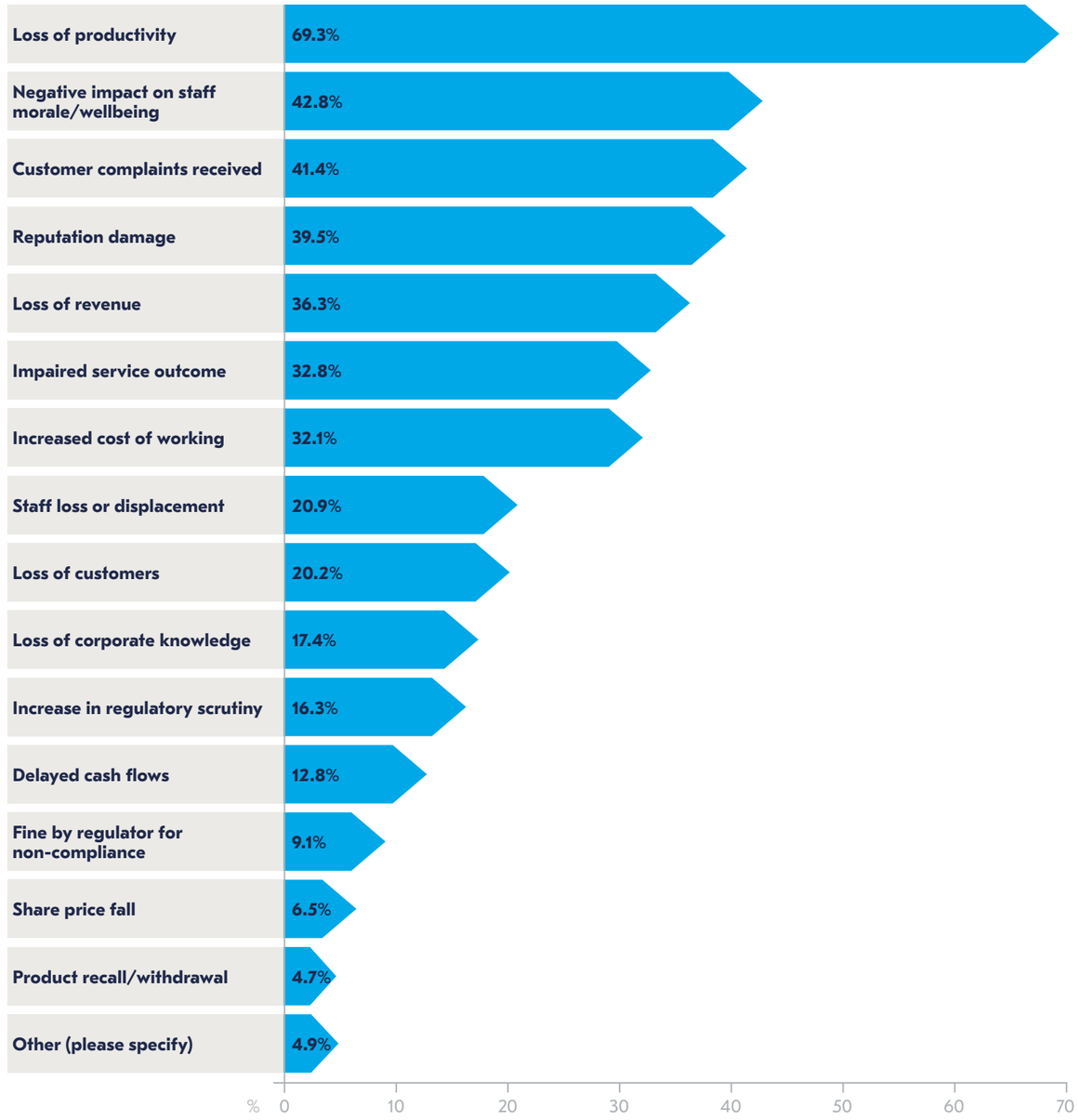


Figure 5. Impacts or consequences arising from the disruptions experienced in the last 12 months

The financial cost of disruption

The financial cost of disruption

- **Regulatory changes top the list in terms of the average cost of disruption at €1.98m. This was the primary financial cost for 29.3% of banking and finance respondents.**
- **Safety incidents rank second at €1.53m, driven up by the high costs associated with work-related fatalities.**
- **Natural disasters and extreme weather also cost organizations over €1m per incident. Whilst many organizations may be able to cover some or all costs through insurance, many organizations in developing countries do not have the funds to insure themselves against such incidents.**

The financial costs associated with disruptions vary significantly between organizations. For example, if a data breach is discovered quickly and managed well, the costs to an organization can be negligible. However, some large scale disruptions can amount costs which have the potential to cripple organizations. The British Airways cyber breach in 2017 earned the company a £187m fine from the Information Commissioner's Office (ICO) when an estimated 500,000 customer credit card details were stolen. It was the largest fine issued to date by the ICO and represented 1.5% of BA's global turnover in 2017[10]. Although British Airways was able to absorb the financial impact of the breach, it could send a smaller organization into bankruptcy.

The average cost of a cyber-attack or data breach was €0.75m in the past year. Whilst large scale disruptions such as the British Airways breach may attract the headlines due to the heavy fines attached, the majority of disruptions are smaller and the resultant costs are less.

> **"I think GDPR is a big player in this because data breaches have the potential to cost organizations a massive amount of money. The fine is based on a percentage of annual turnover. It could equate to some huge fines to organizations who don't have a keen view on how they protect their information."**
> **Business Continuity and Crisis Manager, Financial Services, United Kingdom**

Respondent data from this year's report has allowed us to determine the average cost per each disruption type. Whilst disruptions such as earthquakes or cyber-attacks might be expected to top the table, it is regulatory changes which cost organizations the most per disruption (€1.98m).

The financial services sector is the one most affected by the costs of regulatory changes: 29.3% of financial services institutions reported this category as their most costly disruption over the past year.

Safety incidents rank second in terms of average cost of disruption (€1.53m). The United Kingdom's Health and Safety Executive produced statistics showing 1.7% of the UK workforce suffered a workplace-related injury in 2017/8, costing organizations £5.2bn in total[11]. A fatality costs an organization £1.7m on average and, with 4,600 patient deaths in the UK linked to safety incidents, the risk to organizations is far from negligible[12].

Natural disasters and extreme weather events are the two remaining incidents that cost organizations over €1m on average at €1.07m and €1.00m respectively. The 2019 BCI Supply Chain Resilience Report[13] revealed that many organizations rely on their insurance policies to cover them in the event of a disaster. However, flooding in the UK this year saw many organizations face a large excess payment to cover their losses, with others discovering too late that their insurance did not provide coverage for flood-related claims[14]. For organizations in developing countries, insurance is scarce: Typhoon Mirinae in 2009 triggered losses of US$280m in Vietnam — yet only 3.6% of those losses were insured[15]. It is vital that professionals have recovery plans to mitigate losses and concurrent disruption from such events, not just for their own organization but also amongst their critical supplier network.

It should also be noted that whilst IT and telecoms outages were in second place in this year's risk index, the average cost per incident (€189.2k) places it as ninth in terms of average cost. This should not be an indicator of severity, however given the frequency organizations encounter this type of disruption the financial impact cannot be ignored.

Whilst some organizations account for the costs of disruption very accurately, other organizations fail to fully quantify the full financial burden of individual incidents on the organization. For most, this is through lack of time and resource, particularly if indirect costs are to be considered as well.

10. Calder, Simon 2019, What is the British Airways Data Breach and How Does It Affect Passengers? The Independent, accessed 7 February 2020 independent.co.uk/travel/news-and-advice/british-airways-data-breach-privacy-details-leak-iag-cathay-pacific-information-commissioner-a8993331.html
11. Health and Safety Executive 2019, Costs to Great Britain of workplace injuries and new cases of work-related Ill Health — 2017/18, HSE, Accessed 7 February 2020 hse.gov.uk/statistics/cost.htm
12. Proctor, Kate & Perraudin, Frances 2019, Deaths of 4,600 NHS patients linked to safety incidents, The Guardian, Accessed 7 February 2020 theguardian.com/society/2019/dec/08/deaths-of-4600-nhs-patients-linked-to-safety-incidents-says-labour
13. The BCI 2019, Supply Chain Resilience Report 2019, The BCI, Accessed 7 February 2020 thebci.org/resource/bci-supply-chain-resilience-report-2019.html
14. Peachey, Kevin 2019, England flooding: Why insurance may not cover damage, The BBC, Accessed 7 February 2020 bbc.co.uk/news/business-50391494
15. United Nations Development Programme (UNDP) 2017, Disaster Risk Insurance, UNDP, Accessed 7 February 2020 undp.org/content/dam/sdfinance/doc/Disaster%20Risk%20Insurance%20_%20UNDP.pdf

> **"The priority is to get back to business-as-usual after an incident occurs, so that takes time and resources that are not spent on planned operations. This causes delays in time to market of improved or new services or it causes additional costs. Sometimes we pay fines to our B2B customers because we could not deliver services agreed. Currently from a BCM perspective we do not calculate all losses after an incident, due to a lack of resources and/or automated integrated reporting on those aspects."**
> Business Continuity Officer,
> Telecoms, North West Europe

> **"Financial loss resulted mainly from redirection of resources from "business as usual" to the "unusual", due to the nature of the events. We have not done any analysis on the cost of the down time due to power outages, cyber-attacks or other events. This may be something we would consider in the future."**
> Resilience Analyst, Local Government,
> New Zealand

Average cost of disruption (single incident)

	Disruption	Avg/disruption (€000)
1	Regulatory changes	1982.50
2	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	1525.00
3	Natural disasters (earthquakes, tsunamis, etc.)	1067.86
4	Extreme weather events (e.g. floods, storms, freeze, etc.)	1003.00
5	Cyber attack & data breach	745.00
6	Interruption to utility supply	625.00
7	Political violence/civil unrest	587.50
8	Interruption to utility supply	236.84
9	IT and telecom outage	189.23
10	Critical infrastructure failure	155.00

Figure 6. Average cost of disruption (per single incident)

Benchmarking business continuity

Benchmarking business continuity

- **More organizations now have a Business Continuity Management System certified to the ISO 22301 standard (20.5%)**
- **Organizations who report being certified to the ISO 22301 standard also reported fewer incidents over the past 12 months.**
- **Many organizations choose to align to multiple standards rather than get certified to a single standard.**

There has been a visible uplift in the number of organizations aligning to the ISO 22301 Business Continuity Management standard in 2019. This year, 71.0% of organizations report being certified to ISO 22301 *or* using the standard as a framework: the highest recorded by the Horizon Scan Report since the introduction of the standard in 2012. In addition, if those who use the standard as a framework are stripped out, over a fifth (20.5%) of organizations surveyed report being certified to it; an increase of 6.5 percentage points on 2018.

A further 7.2% plan to move towards certification in 2020, whilst 16.8% have no intention of aligning to the standard over the next twelve months.

Table 1: Percentage of organizations certified or aligning to ISO 22301

Year	Percentage of organizations certified to ISO 22301	Percentage of organizations certified to ISO 22301 OR using it as a framework
2016	11.6%	67.7%
2017	9.6%	65.8%
2018	13.8%	69.2%
2019	20.5%	71.0%

It is the unregulated sectors which are most likely to be certified to ISO 22301: 34.2% of respondents from manufacturing organizations and 33.3% from IT organizations, for example, report their organizations are certified to ISO 22301. Just 16.7% from the financial services sector, however, report similar. Typically, whilst those in regulated sectors might use ISO 22301 as a best practice framework for business continuity, they feel there is less of a need to get certified due to their own industry's regulations which they must adhere to.

Whatever an organization's reasons for certification, organizations that get certified to ISO 22301 have fewer incidents happen during the year: 29.0% of organizations that are ISO certified encountered 11 or more incidents in the past 12 months, whereas 39.8% of those without certification reported 11 or more incidents occurring in the last 12 months — a more than 10 percentage point difference. Such figures could certainly be used by organizations who are struggling to get management buy-in for certification to the ISO 22301 standard.

Do you use any other management system standards to manage risk? If yes, please specify which:

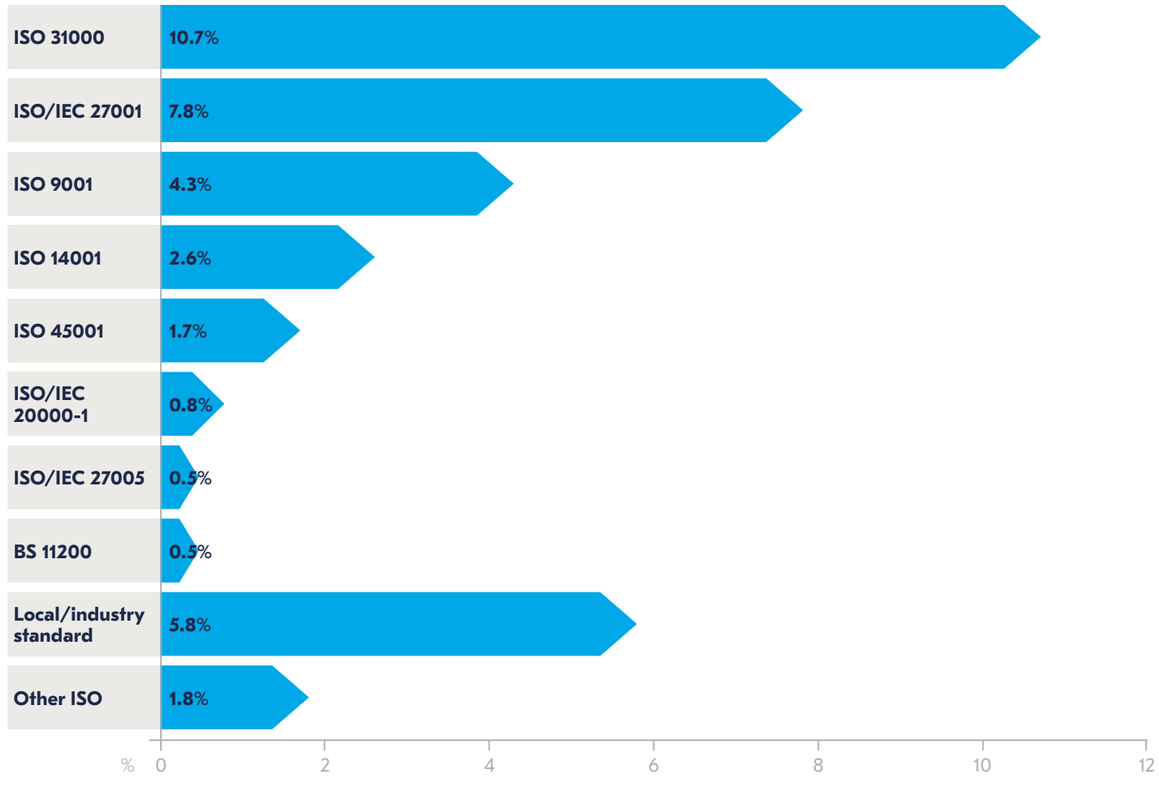


Figure 7. Other management system standards used to manage risk

One of the reasons why organizations choose not to seek certification to ISO 22301 is because they align themselves to multiple standards and find they cannot justify the cost of certification to multiple standards. For those surveyed, the most cited standard used other than ISO 22301 was the Risk Management standard, ISO 31000 with 10.7% of respondents using this within their organization. The Information Security Systems standard (ISO/IEC 27001) was the second most popular alternative standard used (7.8% of respondents) followed by Quality Management Systems (ISO 9001) at 4.3%. Many respondents reported either aligning or getting certified to appropriate country or industry-specific standards.

"I use several ISO standards for guidance and reference, such as ISO 38000 for governance, ISO 27031 for more detail on disaster recovery. ISO 31000 for risk management and ISO 20000 for ITIL. I therefore take all these into consideration with ISO 22301, and BCI's GPG 2018, when setting up the continuity management system and framework within the company."
Business Continuity Officer, Telecoms, North West Europe

What benefits does certification provide to you and your organization?

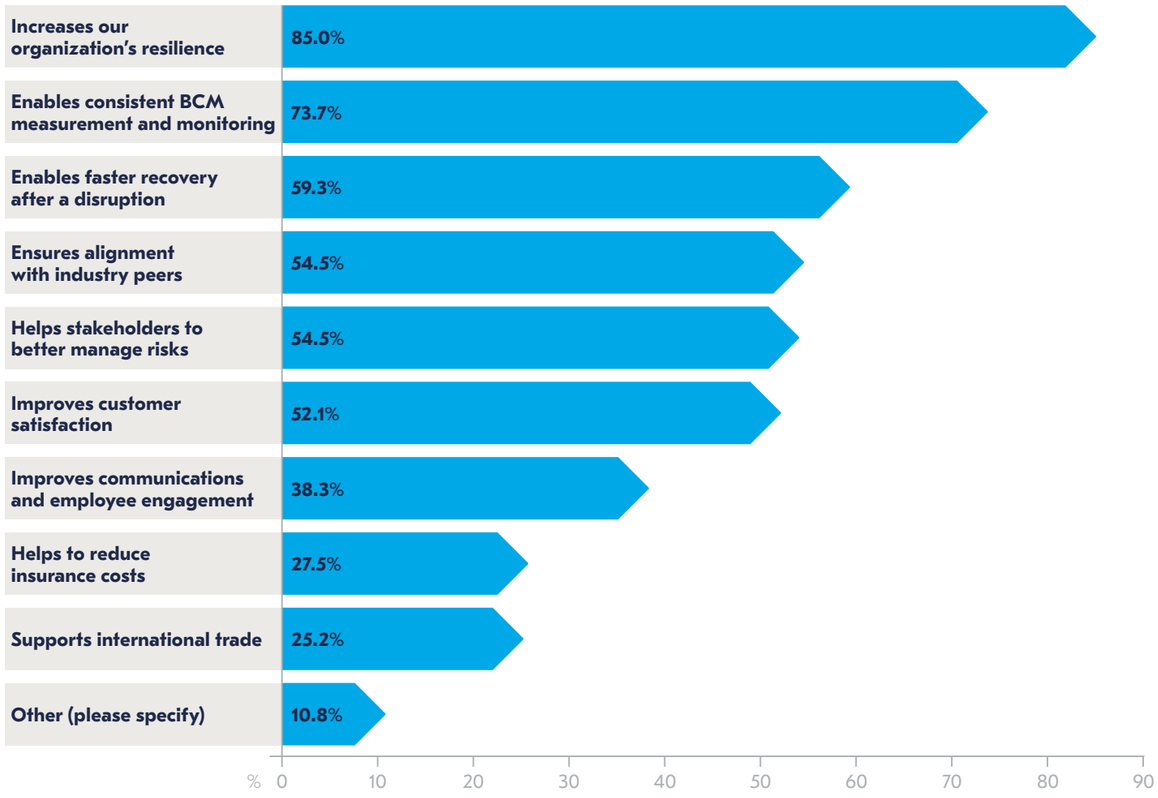
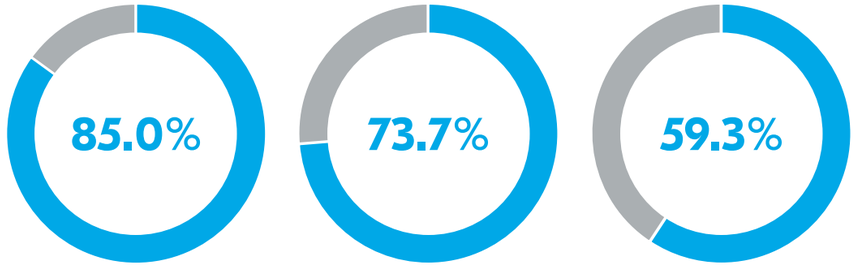


Figure 8. Benefits certification provides to organizations

Getting certified to the ISO 22301 standard not only helps increase the resilience of an organization, but can also benefit the balance sheet

Those who have obtained certification to ISO 22301 highlighted the following as their top reasons for certification:



In addition, more than half reported that it helped to improve customer satisfaction, demonstrating the importance of using the standard within marketing and PR-related activity. Over a quarter (27.5%) claimed that certification helped to reduce insurance costs, whilst 25.2% claimed it helped to support international trade. These three options combined suggest certification can help to boost the balance sheet of an organization. Organizations should investigate how these benefits could be applied to their own organization, particularly where the benefits of certification need to be sold to management in order to get buy-in.

"We've realized significant benefit from being ISO 22301 certified. The certification provides assurance to our customers and our board of directors that we are able to sustain operations when disruptions occur. Our businesses provide critical services to our customers and as our customers' supply chain management maturity has grown, the volume of enquiries has also grown. The certification simplifies our response process and has proven to be very effective in meeting our customers' expectations."
IT Resilience Manager, Publishing, United States

"When we are dealing with incidents with companies who aren't well-prepared from a business continuity standpoint, the costs and the amount of time and effort involved in handling those cases is significantly higher. So, when we're assessing the risk, if a company can adequately demonstrate that they have good business continuity management processes in place, then that will lead to a reduction in premium.

This is particularly the case for larger companies, and we routinely dig deeply to see what they have in place around business continuity - which includes looking for certification to standards such as ISO 22301 and whether plans are regularly tested. The more evidence that the company is able to provide to back up what they do, the greater confidence we can have in that company and the more likely we are to offer more favourable terms."
Stephen Ridley, Cyber Underwriting Manager, Hiscox

Figure 9. Organizations' business continuity management programs and their relationship to ISO 22301

Most organizations value the ISO 22301 standard, but many choose not to obtain certification

The primary reason given by 56.6% of respondents for not obtaining certification to ISO 22301 is due to no business requirement. Just over a third (35.1%) cited there were no external drivers to warrant certification, whilst a lack of management commitment and lack of budget were selected by just under a third of respondents each (28.3%). As mentioned previously, some organizations in regulated sectors felt it unnecessary to adhere to the standard due to having to comply to strict industry regulations.

> **"[Being certified to] ISO standards might get you more business or it could be a prerequisite in getting new business but, for us in the financial services sector, that doesn't happen. Although we align ourselves to the standards, there are very few financial services organizations I've worked in or know of that have seen the value in [certification]."**
> **Business Continuity and Crisis Manager, Financial Services, United Kingdom**

Whilst many organizations may choose not to obtain certification to the standard, many organizations continue to use the standard as a framework, particularly where significant cost controls are in place. Given just 5.8% of organizations feel that the standard is not aligned to their business, the standard is clearly valued and well aligned to organizations' needs.

> **"As a former certified implementer of ISO 22301 I am familiar with the requirements of the standard and we are aligning the processes here at [the] District Council to the standard. We use ISO 22301 as a framework as it shows and shares best practice in business continuity for an organization."**
> **Resilience Analyst, Local Government, New Zealand**

There was also some concern amongst organizations that whilst they could clearly see the value in aligning to a standard, the reputational risk of losing certification to that standard was considered too great by senior management with alignment being the preferred option.

> **"We have our own internal audit function to carry out audits 3-4 times a year against what we say we're going to do in our business continuity program with reference to ISO 22301. We don't think that certification will add too much of an additional cost, but the bad thing for us would be the reputational risk of losing the certification. We therefore like the standard and use it to carry out audit measures against that, but we will not certify against it."**
> **Business Continuity Manager, National Government, United Kingdom**

What are your reasons for not being certified or having no plans to be certified to ISO 22301? Please select all that apply.

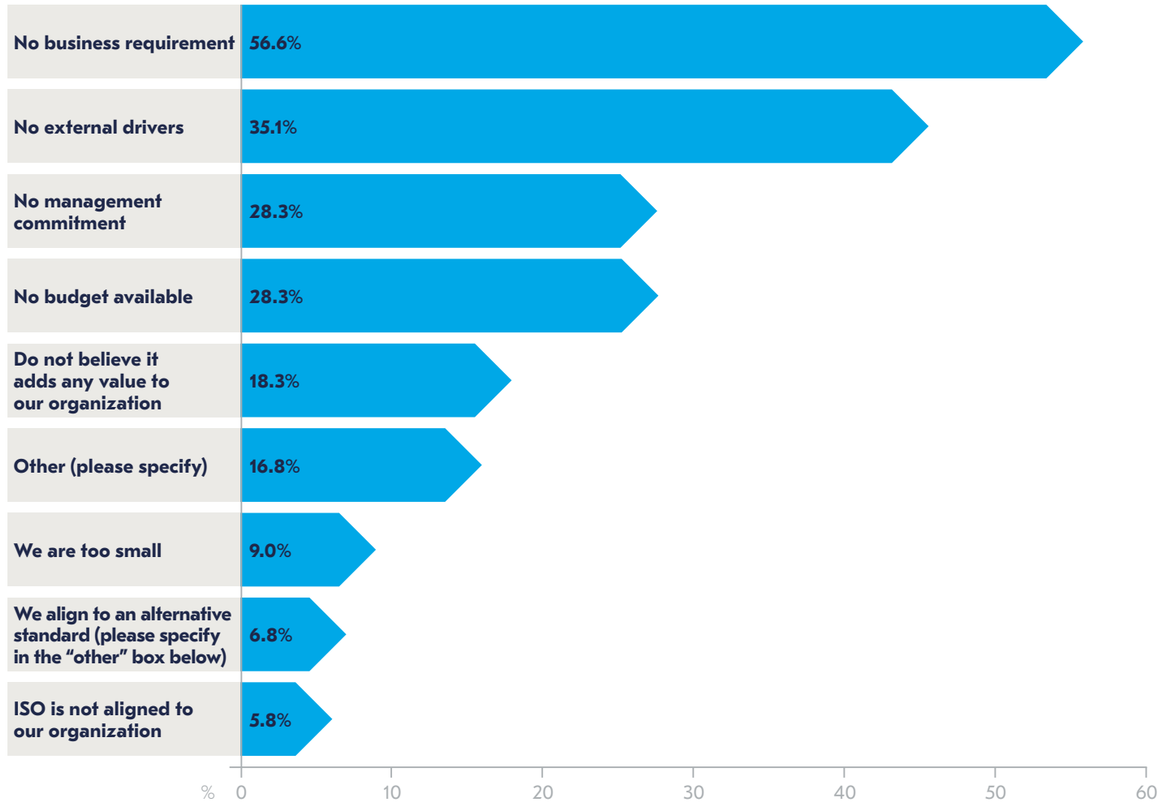


Figure 10. Reasons for not being certified or having no plans to become certified to ISO 22301

Benchmarking longer-term trend analysis

Benchmarking longer-term trend analysis

- **Fewer organizations than last year claim to conduct longer-term trend analysis.**
- **Organizations are increasingly using multiple resources (both internal and external) to form a more holistic view of the threats facing their organizations.**
- **Some professionals report being denied access to the information they need to do effective long-term trend analysis.**

There has been no improvement in the number of organizations conducting longer-term trend analysis, with a total of 76.9% of respondents reporting they carried out this type of analysis compared to 78.0% in the 2019 report. The proportion of organizations conducting centralized analysis has fallen to 45.9% (2018: 52.0%).

Reassuringly, some of the organizations spoken to as part of this report discussed how they get input into their long-term trend analysis work from multiple departments and, in some instances, external experts in order to get a holistic analysis.

> **"You need someone centrally to manage this obviously. The trend analysis needs to be done departmentally or even geographically and using people, amongst others, who are experts within the industry who have a better knowledge than anyone within an internal team. You need to be able to work with that and as the needs of the business changes, be aware that the risk landscape is going to change."**
> **Global Business Continuity Manager, Technology, United Kingdom**

> **"Within our company, we have a strategy department that does the long-term horizon opportunity and threat scanning. The risk department aggregates this with information from all business units and makes a top 10 out of it, so board level can focus on the top risks. We also get intel from other sources. From a business continuity perspective, we can use this information when needed. We constantly improve our capability to prepare our resilience on forecasted threat landscapes."**
> **Business Continuity Officer, Telecoms, North West Europe**

Figure 11. Percentage of organizations using longer term trend analysis to better understand the risk landscape

In addition to noting that longer-term trend analysis is being increasingly carried out on a departmental rather than organizational basis, the survey also indicates that 26.5% of business continuity professionals are also increasingly finding they do not have access to the necessary tools to carry out longer term trend analysis. Encouragingly, two-thirds (67.2%) do have access to this type of information with 22.6% helping to develop the analysis in the first place.

Whilst professionals may feel they do not have a view of their organization's longer-term trend analysis, there are plenty of free resources available to professionals should they wish to do their own risk scanning. Whilst this Horizon Scan Report is one such example, most countries also produce their own country-specific risk register which can be applied to individual organizations. In the UK, for example, there is the National Risk Register of Civil Emergencies[16], the United States has the Homeland Security National Risk Characterization[17] and Australia the National Emergency Risk Guidelines[18]. The OECD also publishes a cross country perspective of risk assessments for its 20 member countries[19].

Different departments may be invited to fill in their own risks for an enterprise-wide risk register, however the register is typically owned by the risk department or, in smaller organizations, by the financial director or accountant[20]. Nevertheless, in order to produce an effective business continuity plan, sight of future risks to the organization can be useful for the business continuity professional.

"In a previous role in the public sector, I noticed when managing the Business Continuity programme that departments and organizations did not always share both departmental and corporate level risk assessments, with many managers being unaware of the corporate risk register and the risk and assurance department worked in silo and was not always forthcoming with risk assessments. In some circumstances, risk governing boards often were disbanded and left other boards to take on the risk assessment role but as a result would fall by the wayside."
Business Continuity Manager, Public Sector, United Kingdom

Many organizations are now looking beyond their own organization and using intelligence from third parties to build a more holistic picture of future risks. In addition to using national and regional risk registers, many look at sectoral risks, risks encountered by peers and suppliers as well as those by businesses located in the area. Even if a business continuity professional does not feel they have access to certain internal information, such external risks can be harvested at no cost.

"We have set out a framework for identification of risk. This covers a description of risks, how each risk should be measured and what we would expect to happen in terms of those risks being escalated up or down the list. We're looking at this now and it needs to happen, as well as an escalation framework built, guidance issued and methodical approach taken."
Business Continuity Manager, National Government, United Kingdom

"I think threat analysis should be carried out and there should be a clear movement of information around all the areas of your organization. I believe we should be carrying out the threat analysis to see what's happening and we do that, looking at our own internal risks, sector risks and sector issues. We also base it on the government risk registers for the UK and Scottish governments."
Business Continuity and Crisis Manager, Financial Services, United Kingdom

"We speak to our third-party suppliers such as our workplace recovery providers and ask them what issues they're seeing and what kind of incidents are making people use their sites. We also tap into our board's risks, we see what people are escalating up the lines from the different businesses and include within our wider risk register and threat analysis."
Business Continuity and Crisis Manager, Financial Services, United Kingdom

16. Cabinet Office 2017, National Risk Register of Civil Emergencies, Cabinet Office, Accessed 7 February 2020 assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf
17. Willis, Henry et al, Homeland Security National Risk Characterization, Rand Corporation, Accessed 7 February 2020 rand.org/pubs/research_reports/RR2140.html
18. knowledge.aidr.org.au/media/2030/handbook-10-national-emergency-risk-assessment-guidelines.pdf
19. Australian Institute for Disaster Resilience 2015, National Emergency Risk Assessment Guidelines, Australian Institute for Disaster Resilience, Accessed 7 February 2020 oecd-ilibrary.org/governance/national-risk-assessments_9789264287532-en
20. Morton, Tony 2010, The Basic Principles of Compiling a Risk Register for Smaller Companies, ACCA, Accessed 7 February 2020 web.actuaries.ie/sites/default/files/erm-resources/tech_afb_trr.pdf

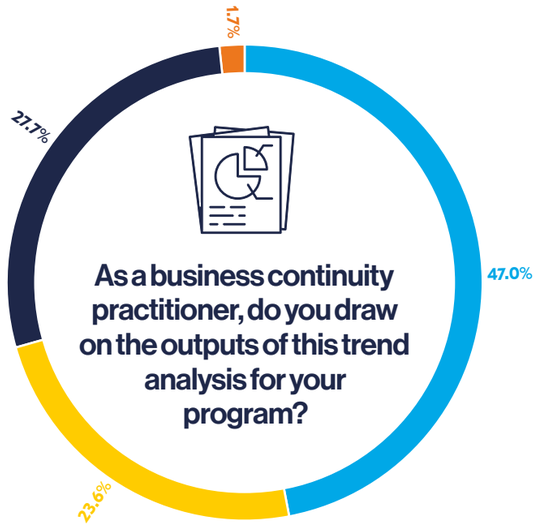


Figure 11. Percentage of organizations drawing on trend analysis outputs for business continuity programs

Internal risk and threat assessment remains the most favoured method of conducting trend analysis, although there is a five percentage point dip on the number reported last year (86.0% down from 91.0% in 2019). Risk registers are at second place (62.5%, down from 71.0% in 2018). This year, all categories have a lower rating than last year which is the opposite to what our qualitative research is telling us. A reason for this could be that many organizations are now using such an array of resources (including organization-defined approaches), and the use of more traditional techniques is waning as a result.

> **"We do look at what has happened to similar organizations in the previous year or five years and look to central bodies and organizations such as the Local Government NZ (LGNZ) and Society of Local Government Managers (SOLGM) to assist with this. We also review the realities of the world we are currently in and find the news is a great source of information. One area we are reviewing this year will be around insurance as during the first two weeks of our new insurance policy the UK flooded, one of our large corporations had a fire and Australia started to burn. We've also had a volcanic eruption in NZ, and the ramifications have caused implications not only to the people involved but also to the wider area and its economy."**
> Resilience Analyst, Local Government, New Zealand

> **"We look both internally and externally, looking at internal risks as well as external information such as risk registers or key threats identified by the big four as well as key information identified by regulators. We look at government risk registers as well as reports such as the BCI Horizon Scan Report. We also have forums where our cyber threat intelligence people talk to other people in the same sector and use that to learn and protect, although these tend to be less widely spoken about, even within the organization."**
> Business Continuity and Crisis Manager, Financial Services, United Kingdom

> **"We do look at some external sources such as general news, media websites; especially those sourced from our external media team. But most of it is done internally and therefore requires a reliance on internal knowledge."**
> Global Business Continuity Manager, Technology, United Kingdom

How do you conduct a trend analysis of the risks and threats to your organization?

Figure 12. Methods organizations use to conduct trend analysis of risks and threats

12.2% of respondents to this year's survey report that their organization has only been engaged in business continuity management planning for a year or less, with a further fifth (21.7%) only having a program in place for the past 2-3 years. This could also go some way to explain the relatively low level of responses for all trend analysis techniques as many organizations are still embedding the process.

12.2%
1 year — this is still new for the business

21.7%
2-3 years — this has been recently established

17.0%
3-5 years — this is a well-established programme

49.1%
5+ years — this is a mature programme

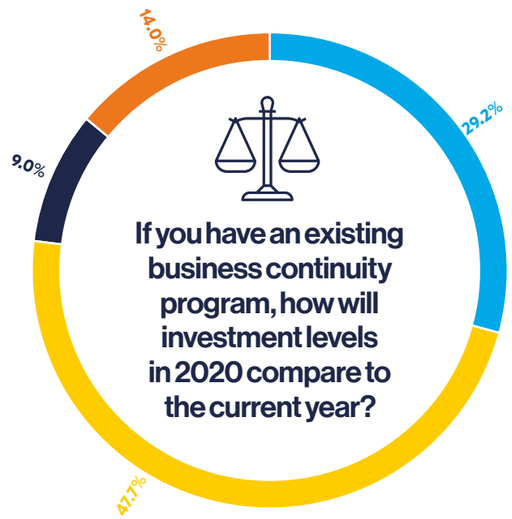
Figure 13. Length of time organizations have been engaged in business continuity management planning

When considering investment in existing business continuity programmes, 28.1% of respondents said that investment will be increased to meet the needs of a growing program (2018: 29.0%). 47.7% said that business continuity investment would remain the same over the next year, a slight fall on the 53% reported in last year's edition. This fall, however, is likely to be attributable to the rise in the number of respondents who were unclear on the investment intentions of their organization: this year, 14.0% of respondents were unclear on investment intentions compared to 9.0% in the previous year.

Nevertheless, with many global economies facing uncertainties over the next 12 months, it is encouraging that just 9.0% of organizations report that investment in business continuity programs will fall over the next year (2018: 8.0%).

Many of those surveyed reported they were being diligent at proving the value of business continuity to management which was helping them to get additional budget for their programs. Others reported using the term "resilience" rather than "business continuity" was helping them to achieve more organizational buy-in for their programmes.

"The usage of business continuity planning as a justification for doing or not doing something has increased - sometimes for good reasons, sometimes for less good reasons - but certainly the language is there in the vocabulary of how we do things. People are also talking more about resilience, which is something we're doing. We're using that word as an umbrella for our risk, crisis, and BC stuff. The language of BC has become more prevalent [when investment decisions are made]."
Business Continuity Manager, National Government, United Kingdom



29.2%
Investment will be increased to meet the needs of a growing programme or new requirements.

47.7%
Investment will be maintained at appropriate levels for the programme scope and position in the lifecycle.

9.0%
Investment will be cut, limiting the scope or effectiveness of the programme.

14.0%
I don't know.

Figure 14. Business continuity program investment levels in 2020 compared to 2019

Annex

665 Respondents

74 Countries

19 Sectors

9 Respondent Interviews

50.5% Business Continuity

15.0% Risk Management

7.6% IT Disaster Recovery/ IT Service Continuity

4.3% Top Management

3.7% Emergency Planning

2.8% Crisis Management

2.4% Cyber/Information Security

2.0% Quality/Business Improvement

1.8% Internal Audit

1.7% Health & Safety Management

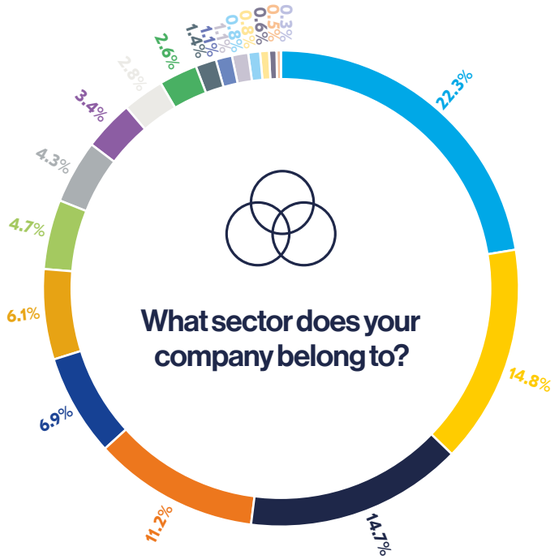
1.4% Security (physical)

0.8% Supply Chain/Logistics/ Procurement/Purchasing

0.2% Line of Business/ Service Directorate

6.0% Other (please specify)

Figure 15. Which of the following best describes your functional role?



22.3% Banking and finance

14.8% Professional services

14.7% Information technology

11.2% Public services, government and administration

6.9% Manufacturing

6.1% Energy and utilities

4.7% Healthcare

4.3% Transport and logistics

3.4% Education and training

2.8% Emergency services

2.6% Retail and wholesale

1.4% Science and pharmaceuticals

1.1% Engineering and infrastructure

1.1% Real estate and construction

0.8% Charity/Not for profit

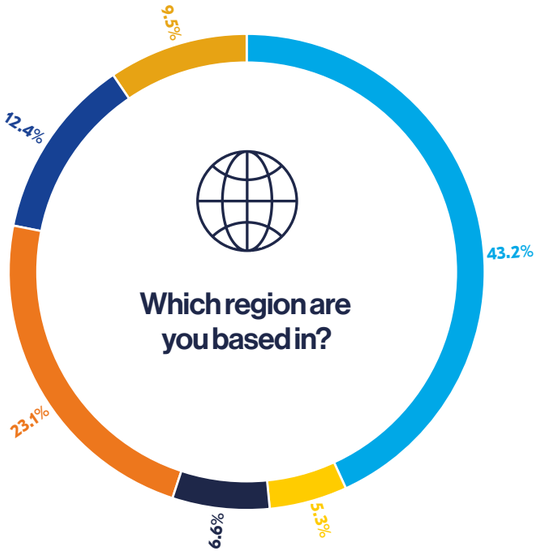
0.8% Law enforcement and security

0.6% Leisure and hospitality

0.5% Creative industries

0.3% Environment and agriculture

Figure 16. What sector does your company belong to?



43.2% Europe

23.1% Americas

12.4% Asia

9.5% Australasia

6.6% Africa

5.3% Middle East

Figure 17. Which region are you based in?

7.3% 1-10

3.4% 11-20

0.8% 21-50

1.4% 51-100

3.8% 101-250

5.2% 251-500

7.5% 501 - 1,000

22.8% 1,001 - 5,000

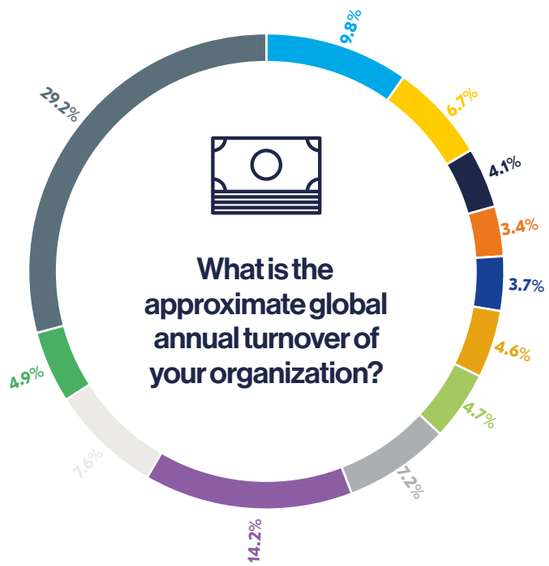
10.4% 5,001 - 10,000

17.9% 10,001 - 50,000

8.2% 50,001 - 100,000

11.5% More than 100,000

Figure 18. Approximately how many employees are there in your organization globally?



9.8% Less than €1 million

6.7% €1-10 million

4.1% €11-25 million

3.4% €26-50 million

3.7% €51-100 million

4.6% €101-250 million

4.7% €251-500 million

7.2% €501 million-€1 billion

14.2% €1-10 billion

7.6% €11-50 billion

4.9% Greater than €50 billion

29.2% I don't know

Figure 19. What is the approximate global annual turnover of your organization?

Asia Pacific: past 12 months

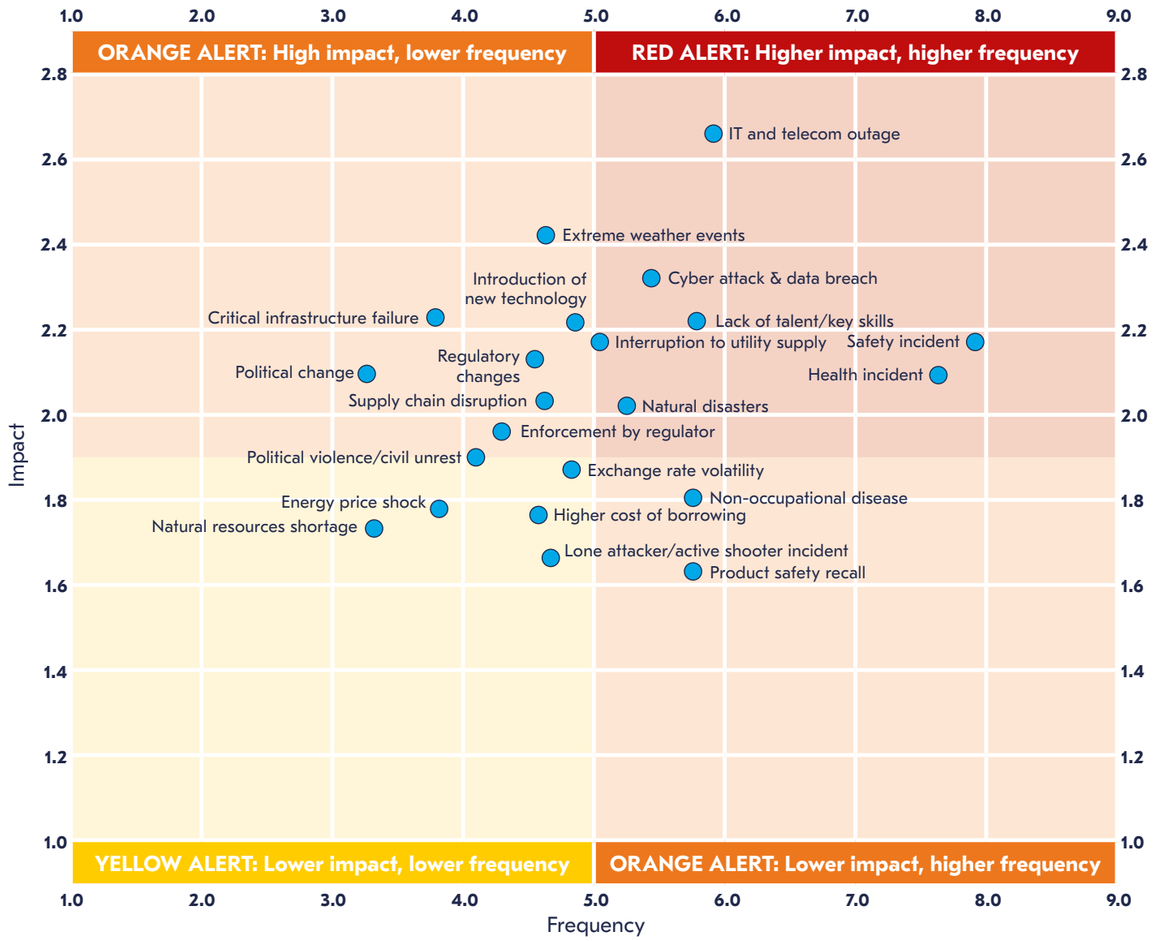


Figure 20. Risk and Threat Assessment: Past 12 Months (Asia Pacific)

Asia Pacific: next 12 months

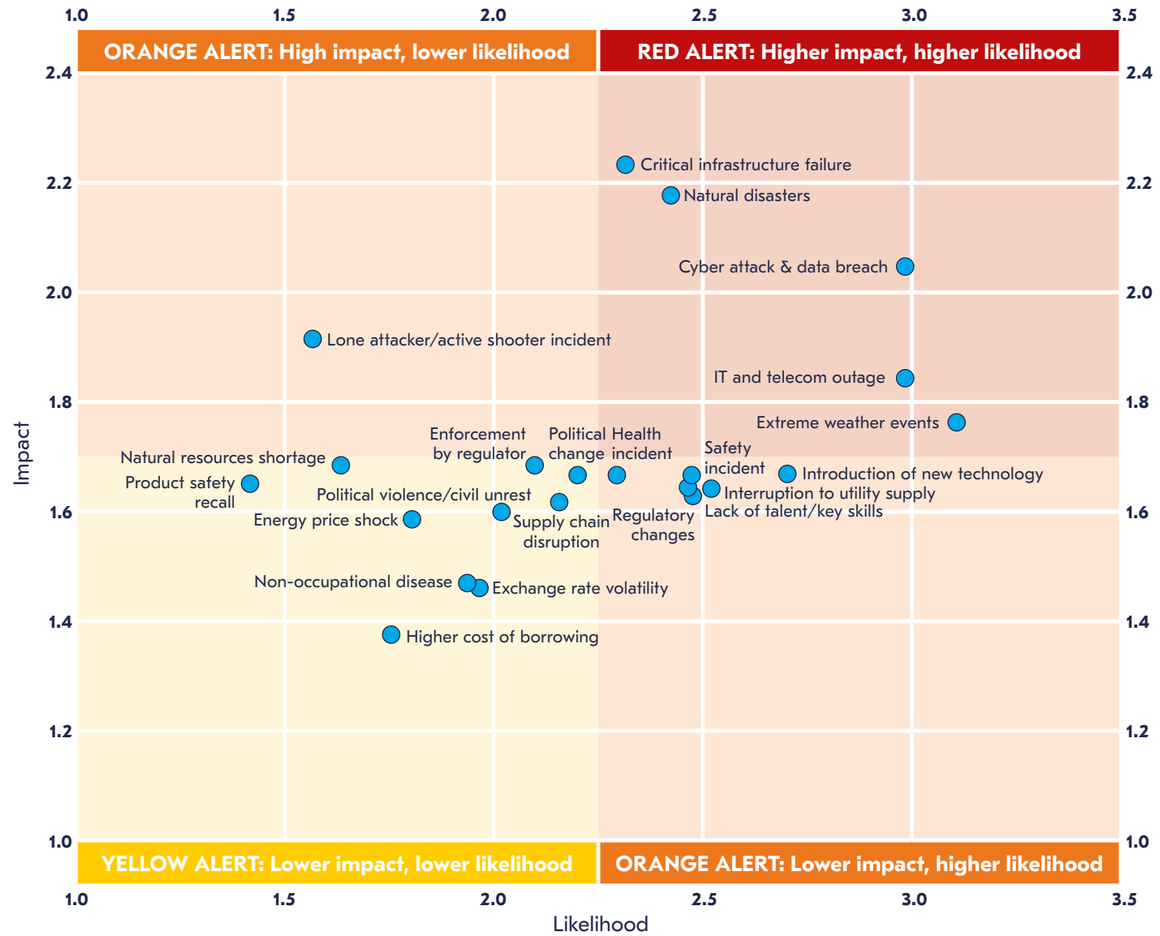


Figure 21. Risk and Threat Assessment: Next 12 Months (Asia Pacific)

Europe, Middle East & Africa: past 12 months

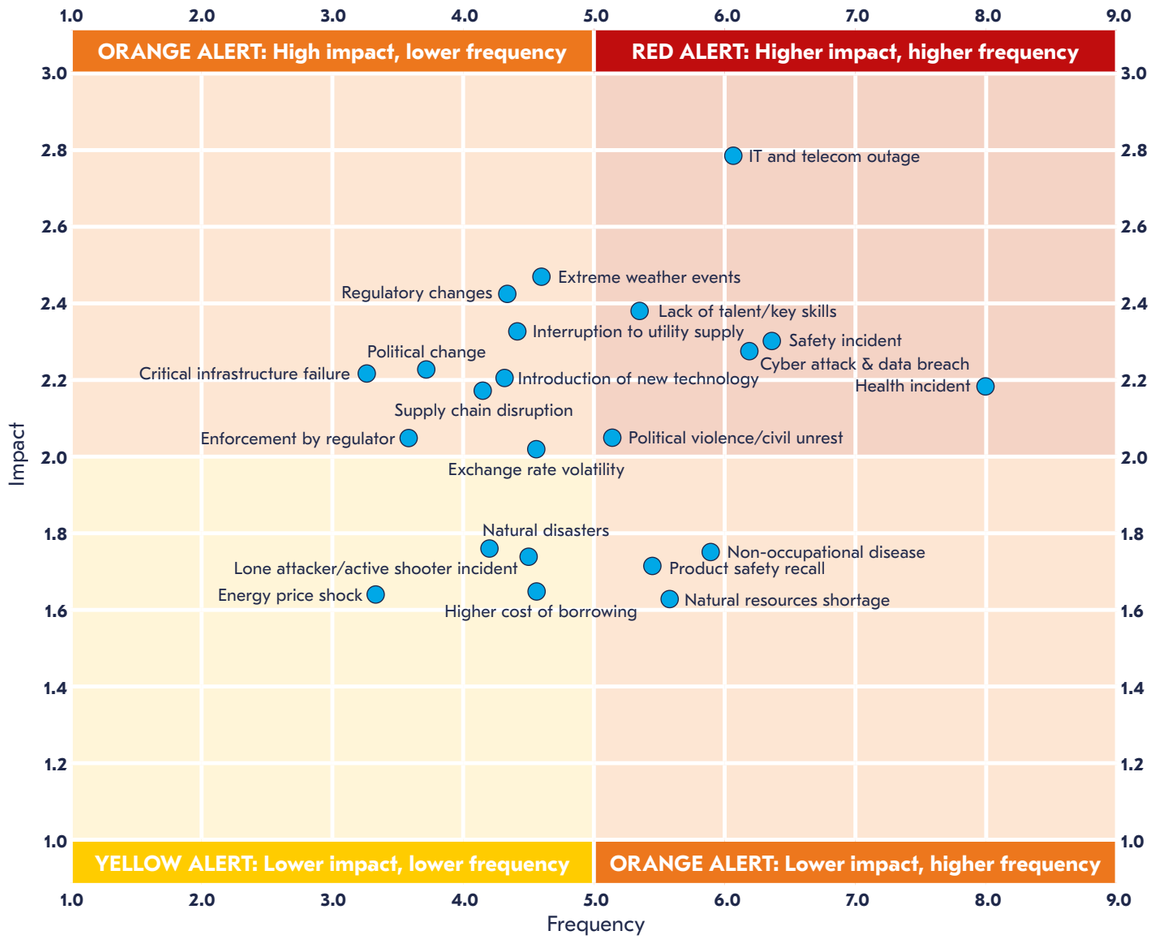


Figure 22. Risk and Threat Assessment: Past 12 Months (Europe, Middle East & Africa)

Europe, Middle East & Africa: next 12 months

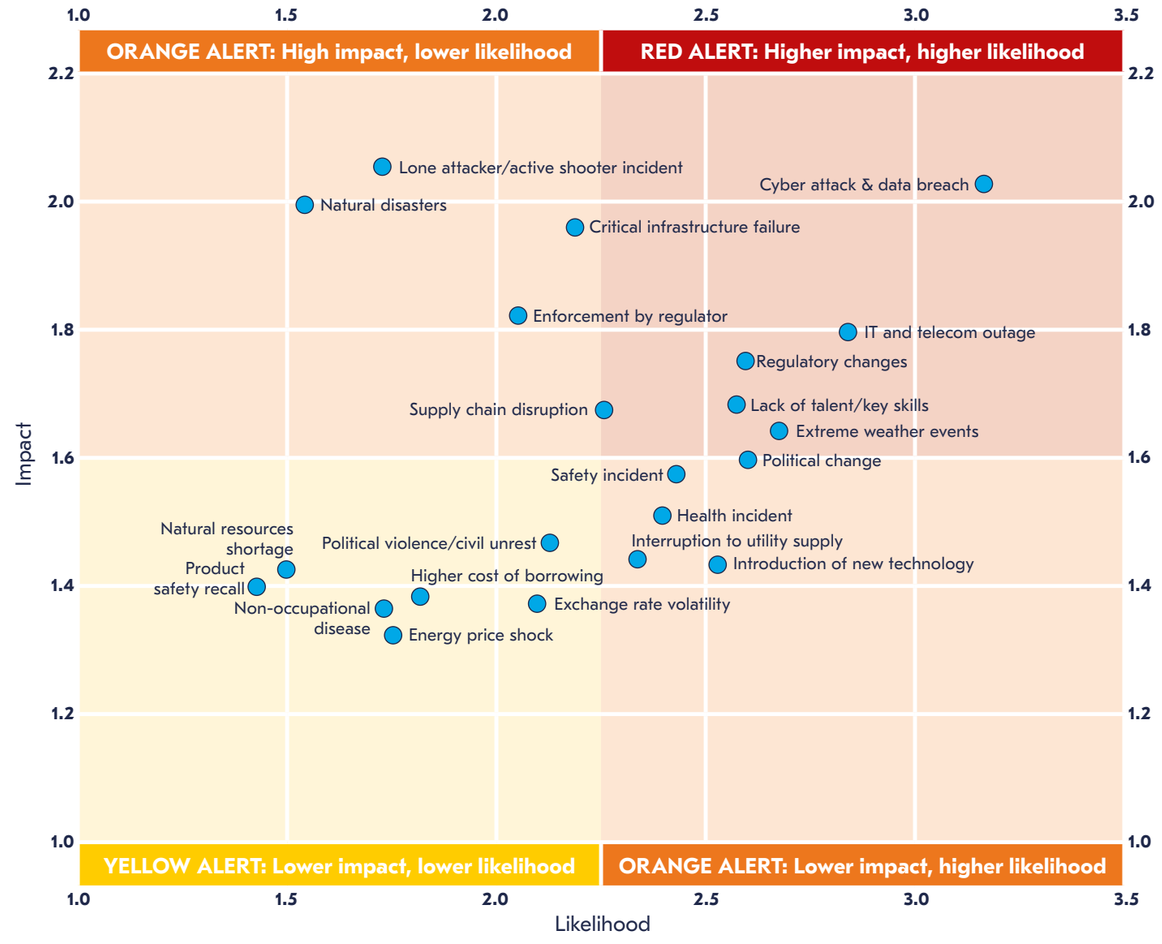


Figure 23. Risk and Threat Assessment: Next 12 Months (Europe, Middle East & Africa)

Americas: past 12 months

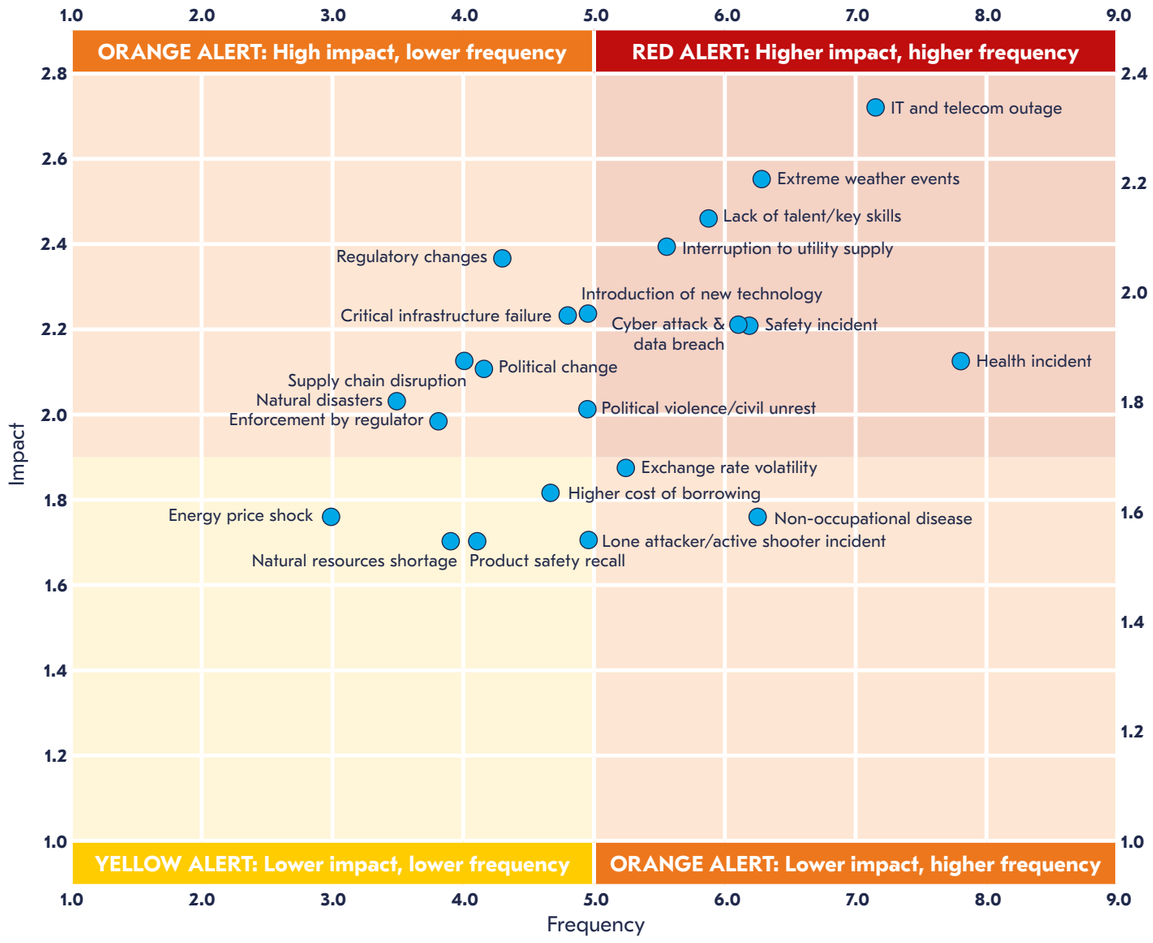


Figure 24. Risk and Threat Assessment: Past 12 Months (Americas)

Americas: next 12 months

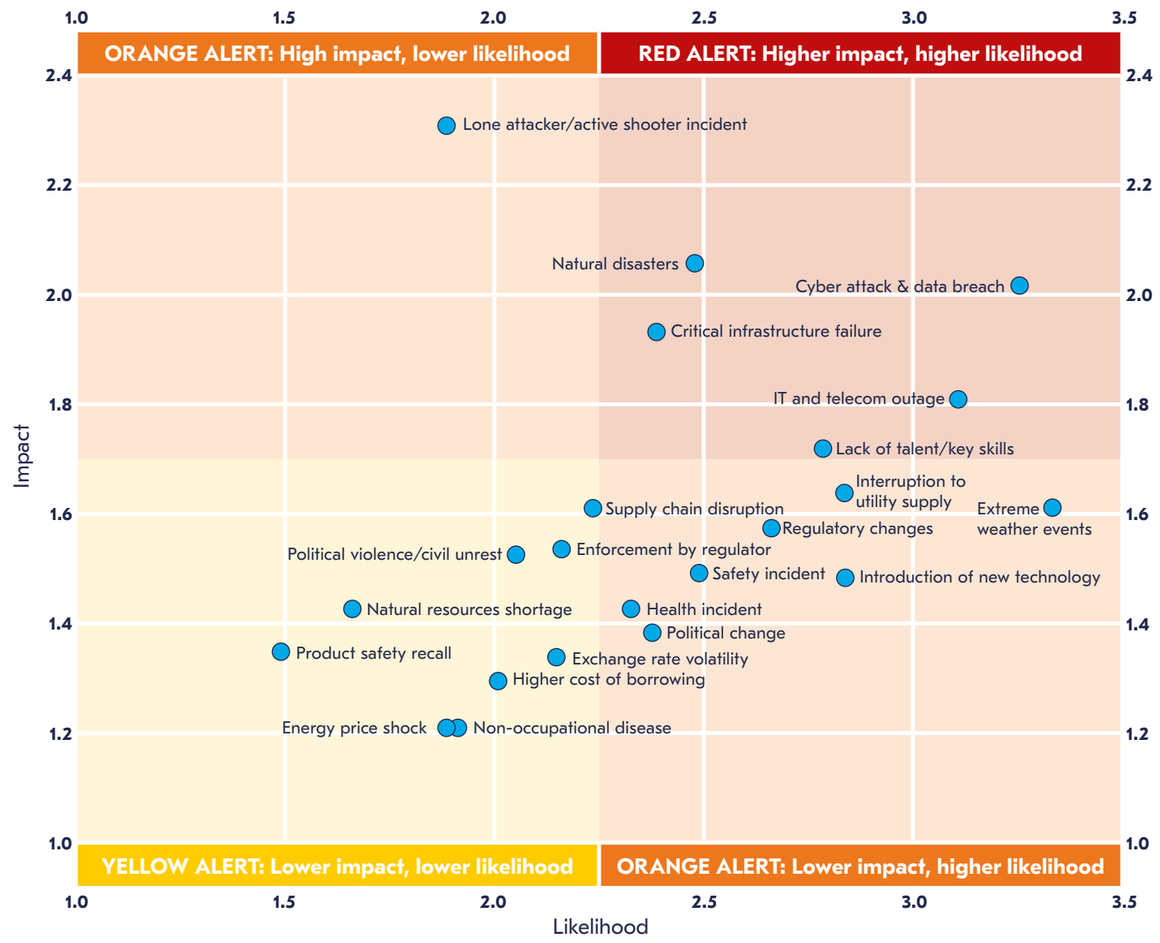


Figure 25. Risk and Threat Assessment: Next 12 Months (Americas)

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

Catherine Thomas MBCI (Research and Insight Manager)

Catherine comes from a resilience background in central and local government with a particular focus in public health and community incident response. She holds a Masters degree in Forensic Investigation from Cranfield University and a BSc in Forensic Investigation from Canterbury Christ Church University. She has a background in research from an analytical and qualitative perspective and has a particular interest in delving into the qualitative detail behind our surveys through investigative research

She can be contacted at catherine.thomas@thebci.org

Kamal Muhammad (Research and Insight Analyst)

Kamal 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

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 9,000 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

+44 118 947 8215 | bci@thebci.org
10-11 Southview Park, Marsack Street, Caversham, RG4 5AF, United Kingdom.

About BSI

BSI is the business improvement company that enables organizations 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 84,000 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, Regulatory Services and Consulting Services, BSI improves business performance to help clients grow sustainably, manage risk and ultimately be more resilient and trusted.

To learn more, and find contact details for your local BSI office, visit www.bsigroup.com

Correct as of February 2020

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

bci@thebci.org / www.thebci.org

bsi.

bci Leading the way to resilience