Find out more
www.thebci.org

Thought Leadership

BCI Horizon Scan Report 2021

bsi.

Leading the way to resilience

Contents

Foreword

I am pleased to introduce the 2021 BCI Horizon Scan report, one of the most established annual reports in our portfolio. We are very grateful for the continuing support of BSI, our longstanding partner in the production of this report.

Over recent years, "traditional" disruptions such as cyber-attacks, extreme weather and IT outages have been firmly positioned at the top of the list of disruptions that have occurred over the past year. Because of the impact these events have on organizations year after year, they also inevitably feature at the top of practitioners' minds as concerns for the upcoming year.

For some organizations, this means preparations for certain risks, threats and events are ignored, even if they are likely to happen and have the potential of causing extreme impact. Michele Wucker famously dubbed these "grey rhino" events, a term which has been familiar with many resilience professionals and has become even more prominent during the pandemic. This past year has been a real-world demonstration of how being resilient and prepared for grey rhino events can be the difference between business survival and business collapse.

Not unexpectedly this report shows that COVID-19 caused severe disruption to organizations in 2020 but, for many, it also provided a timely wake-up call to be better prepared for future crises. The research reveals that organizations are taking a more critical view of future risks and are writing plans for scenarios which have been avoided or neglected in planning up to now. Others are already investing in new technologies to help with risk scanning while others are taking a multifaceted approach, drawing on inputs from other sectors, peers, regional and national governments and industry groups.

The future certainly will not be all about COVID-19, but many practitioners feel unable to remove it from long-term planning and there is concern that new, emerging risks may be missed in the same way COVID-19 was. Climate risk, for example, is no longer something that can be ignored from risk planning. While the visible indicators of climate change such as wildfires, floods and extreme temperatures are already causing operational disruption to organizations, new laws and regulations relating to climate change will need to be followed and in our social media connected world non-compliance could have a devastating reputational impact.

Encouragingly, the disruption during the year has meant many organizations are introducing more robust business continuity programmes. At the BCI, we have seen a strong uptake of our certification courses and skills training, and this survey also reveals that an increasing number of organizations are looking at using the ISO 22301 as a framework for the first time.

2020 may have been a year of extreme disruption, but it has been a year where the importance of horizon scanning has been brought to the forefront. We hope that this year's report continues to serve as a useful benchmarking tool and provides valuable learnings for your own organization. I would once again like to thank the BSI for the continued and valued support of this report.

Christopher Horne FBCI
Chair of the BCI

Foreword

Each year, we ask business continuity and resilience professionals to use their knowledge to provide valuable insight by ranking what they consider to be the most likely future risks.

This latest report provides an expert view of a year that challenged business continuity more than any other. The Covid-19 pandemic caused widespread disruption for many organizations, and this year's results highlight the importance of developing a risk management approach that includes planning for the unexpected to ensure enduring resilience.

In 2019, non-occupational disease was second from bottom of the list; this year, for the first time, it is rated as the top disruption. The secondary impacts of Covid-19, such as health and safety incidents, IT / telecom outages and cyber-attacks have all increased significantly when compared with previous years.

Looking ahead, managing supply chain disruption and ensuring a robust financial position are key focus areas for organizations. Health and safety incidents will continue to be a concern, however it appears cyber-attacks and IT / telecoms outages have slipped down the priority list as organizations have been focused on the pandemic. Organizations will need to continue to focus on business-as-usual risks, which if ignored, could negatively impact their long term resilience.

The report reveals that business continuity and resilience professionals are confident of more investment in business continuity this year and programmes appear to be maturing, which is a good sign. This is also apparent in our 2021 Organizational Resilience Index, which identifies a clear association between having a mature, holistic approach to Organizational Resilience and positive financial performance. Horizon Scanning is a key factor in ensuring a business remains resilient.

As organizations start to build back post-pandemic, best practices such as ISO 22301 and the BS 65000 Organizational Resilience framework can help them to seize the opportunities ahead. Many are also using ISO 22301, the international standard for business continuity management, as a framework to help safeguard their business against future threats, reporting that the standard increases their organization's resilience and ensures faster recovery following disruptions.

BSI has proudly supported the Horizon Scan Report since its launch 10 years ago and it's pleasing to see that more than 70% of organizations are now utilizing these industry reports to help with their risk planning and ensure their organization remains resilient in the future.

Harold Pradal
Group Commercial Director,
BSI

Horizon Scan
Executive summary

Executive summary

The COVID-19 pandemic was more disruptive to organizations than any incident noted previously in the Horizon Scan report.

Non-occupational disease earned a risk score of 18.6 in the risk index for 2020, the highest risk score ever noted in the Horizon Scan reports. One of the primary reasons for disruption was the lack of preparedness by organizations: non-occupational disease was second from last in the list of concerns for 2020 in last year's Horizon Scan report.

The secondary impacts of COVID-19 also pushed other categories up the table for events occurring last year.

Health incidents, another category which was deemed a low risk for 2020, finished the year as the second largest disruptor. Many of these health incidents were not from pathological causes, but from mental health difficulties experienced by staff as a result of COVID-19. Cyber-attacks and IT/telecom outages also caused high levels of disruption in 2020 as a result of elevated cyber-crime. As criminals sought to exploit security holes as staff worked remotely, and unforeseen network outages caused primarily by issues with internet latency.

COVID-19's legacy has meant practitioners are considering new risks in 2021.

Whilst non-occupational disease receives the highest risk score for 2021, the disease has made organizations consider new risks in the year ahead. Political risks and violence has returned to the top 10 in the risk index for the first time in three years, and continued disruption to IT and telecoms service is predicted, particularly as new tools and technology are implemented in the wake of the pandemic.

Climate risk is now the primary medium- to long-term risk for many organizations.

With organizations suffering increasing incidents of extreme weather coupled with new laws and regulations requiring organizations to reach certain targets, climate risk was identified by interviewees as being of highest concern over the medium to long term. Could the next major impact not come from a black swan or grey rhino event, but a Marsh & McLennan dubbed "green swan" event?

Certification to ISO 22301 fell slightly during 2020, but its use as a framework increased.

Many organizations said delayed or missed recertification appointments in 2020 had resulted in their certification lapsing, but hoped to do so before the six month grace period expired. There was, however, an uptick in the number of organizations adopting the standard as a framework during the year, suggesting the impact of the pandemic was causing them to re-evaluate the effectiveness of their business continuity programmes. For those who have had certification lapse recently or have one that is about to expire, contacting the certification provider to discuss options would be advisable.

The number of organizations performing longer-term trend analysis has risen to an all-time high of 81.3% - with over half now carrying it out on a centralized basis.

Respondents reported that COVID-19 had been the precipitator to introducing a more structured, centralized analysis programme into their organizations. Frequently, this drive has come from management who have been more demanding of outputs of trend analysis due to heightened levels of uncertainty.

Risk and threat assessment

Risk and threat assessment — past twelve months

Non-occupational disease is firmly at the top of the table for 2021 with health and safety close behind

Non-occupational disease (e.g. pandemic) was second from last in the list of concerns for 2020 yet ended up being the primary cause of disruption for most organizations

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

Non-occupational disease:
18.6

Health incident:
18.2

Safety incident:
16.1

IT and telecom outage:
15.8

Cyber-attack and data breach:
15.3

Risk and threat assessment — next twelve months

Pandemic concerns continue to dominate for the next twelve months

Disconnects still exist in terms of what has happened and what will happen with professionals' concerns diverted to the risks they feel they have little control over

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

Non-occupational disease:
9.0

Cyber attack & data breach:
6.6

IT and telecom outage:
5.2

Regulatory changes:
5.0

Extreme weather events:
4.8

Consequences of disruption

Staff morale and wellbeing has been hit badly by the COVID-19 crisis in 2020

Staff morale and wellbeing was selected as a consequence of disruption by 61% of respondents — up 20 percentage points from last year's report

Leading impacts or consequences of disruption over the past 12 months

Loss of productivity:
64.8%

Negative impact on staff morale/wellbeing:
61.4%

Loss of revenue:
51.7%

Increased cost of working:
43.6%

Staff loss or displacement:
40.3%

ISO 22301 Update

Nearly three-quarters of organizations are either certified to ISO 22301 or using it as a framework

5% of organizations plan to move towards certification in 2021

Percentage of organizations certifying and/or aligning to ISO 22301

We use ISO 22301 as a framework but are not certified to it:
47.6%

We use ISO 22301 as a framework and are in the process of getting certified:
5.1%

We use ISO 22301 as a framework and certify to it:
12.5%

We don't use ISO 22301 as a framework but will move towards this during 2021:
6.4%

We don't use ISO 22301 as a framework and have no plans to during 2021:
28.3%

Benefits of certification

The majority of organizations certify to increase their organization's resilience and to enable consistent BCM measurement and monitoring

Some organizations also appreciate the financial benefits certification can offer

Benefits of aligning to ISO 22301 (selected statistics)

It increases our organization's resilience:
71.8%

It enables consistent BCM measurement and monitoring:
69.0%

Ensures alignment with industry peers:
56.3%

Helps to reduce insurance costs:
40.9%

Supports international trade:
36.6%

Benchmarking longer term trend analysis

Organizations are starting to look beyond traditional methods when performing a risk and threat trend analysis

Carefully corroborated social media is seeing widespread use in organizations

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

Internal risk and threat assessment:
91.7%

External reports/industry insight (e.g. Horizon Scan):
71.7%

Risk registers:
71.7%

Participation in industry events/conferences:
58.7%

Social media monitoring:
44.4%

Investment in business continuity programmes

Nearly a third of organizations report investment into BC programmes will be increased in 2021

Investment levels in Business Continuity Programmes in 2021

Investment levels will be increased:
30.9%

Investment levels will be maintained:
45.7%

Investment levels will be decreased:
9.1%

Overview

Last year's Horizon Scan report was published at the same time most countries were going into their initial COVID-19 invoked lockdowns. At this point, little was known about how deeply the pandemic would affect the world as well as the longevity of the pandemic period. The 2019 Horizon Scan ranked non-occupational disease as second from last in the risk and threat index for the next twelve months. This year, it has catapulted to the top of the table with the highest risk score ever noted in the Horizon Scan report.

On 31 December 2019, the day last year's Horizon Scan survey closed, global news agencies first reported that the World Health Organization (WHO) had discovered an "unidentified outbreak of viral pneumonia". At that point, 27 people had been treated in hospital and seven were in a "serious condition"[1]. Indeed, the potential global risk did not become apparent to many organizations until the end of January/early February 2020.

However, there were a small number of business continuity and risk teams who had active horizon scanning capabilities in place and tracked the emergence of this "viral pneumonia" at the end of 2019. This enabled them to alert senior management and update plans with the emerging intricacies of the COVID-19 pandemic[2].

The same BCI research revealed that many organizations were taken by surprise at the speed the pandemic took hold. Pandemic plans were found to be built around previous pandemics/epidemics which did not readily adjust to the breadth of the impact of COVID-19 or the intricacies required to illicit an effective pandemic response. As a result, many organizations suffered disruptions with some being hit by irreparable damage.

The pandemic has been a lesson in the importance of horizon scanning and being better prepared for grey rhino events (events which are highly probable and will have a high impact but are overlooked) or black swan events (events which are impossible to predict, have a major effect yet often appear obvious in hindsight). The heavy impact of COVID-19 on organizations means many are already reviewing how they look at the risk landscape: interviews carried out for this report reveal many organizations are now broadening how they look at the risk landscape, taking more consideration of National Risk Registers and writing/rewriting plans for events which had, until now, been considered as unlikely to occur.

1. DW.com (2019). China investigates SARS-like virus as dozens struck by pneumonia. DW.com [online]. Available at: https://www.dw.com/en/china-investigates-sars-like-virus-as-dozens-struck-by-pneumonia/a-51843861 [accessed 24 February 2021]
2. BCI, The (2020). The Future of Business Continuity & Resilience. The BCI. Available at: https://www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html [accessed 24 February 2021]

Risk and threat assessment: past twelve months

Risk and threat assessment: past twelve months

- COVID-19 has pushed non-occupational disease to the top of the risk table for 2020 with the highest score ever noted in the Horizon Scan report.
- Health and safety incidents take second and third place respectively, with mental health driving up the score for health incidents.
- COVID-19 did not suppress other disruptions in 2020: new records were recorded for extreme weather events, and regulatory changes also saw an uptick in 2020. The importance of being prepared for multi-event impacts is crucial.
- Technology and telecoms-related incidents have remained high, with the secondary effects of COVID-19 also causing impacts to organizations (e.g. latency problems, elevated levels of cybercrime, adoption of new technology).

There are few organizations where COVID-19 was not the top cause for disruption in 2020 and equally, there will have been an even lower number of organizations who would have considered that the pandemic would have had the impact it has if they had been questioned prior to the outbreak.

8.4% of Resilience professionals reported being aware of the risk of COVID-19 prior to January 2020[3] due to meticulous scanning of World Health Organization (WHO) data. However, the majority were unaware until the news first broke to the world on 31 December 2019 as a "mystery pneumonia" virus which was so far contained in Wuhan, China[4]. As the virus began to spread around the world, organizations started to activate their Business Continuity plans. At this stage, understanding of the virus was still relatively low, although those organizations with operations in the Far East were able to use experiences from those operations to rewrite and modify plans accordingly.

"From a product point of view, we have operations in China and a distribution centre in China. So, there was a limited amount of sourcing we could do from China. We're not entirely reliant on them, however we do have a sizable staff base over there in China, 400 people, and that helped us to see what difficulty they were experiencing in the initial stage of it and translate those learnings to our operations."

Head of Business Continuity, Electronics, United Kingdom

"We quickly put together a skeletal pandemic plan to go out to all of our offices over the seven days after we decided to watch the threat on the 15 January. We put that together and issued that just to get them thinking about what they might need to do and have something to reference. At the same time, our China offices had already got into full BC mode in terms of what they were doing. One of the offices had taken the lead in terms of the Chinese response and initially we learned a lot from them, quite honestly."

Head of Risk, Healthcare, United States

"Our China operations are phenomenal. As a company, we started watching the pandemic at the end of December. By the first week of January, ahead of the Chinese New Year, China was already preparing for a pandemic response. Since we are a global company, we were able to benefit from their preparation and our collaborative culture. While we were watching what was happening in China in January, our global business services organization was doing scans to make sure that all of our networks and IT infrastructure could handle everyone working from home because this is the strategy that China operations employed. In addition, once we saw the pandemic move to Spain and Italy, our teams in those countries began to inform us about the effect of the pandemic on operations and we formulated the second maturity of the pandemic plan."

Business Continuity Manager,
Consumer Goods, United States

3. BCI, The (2020). The Future of Business Continuity & Resilience. The BCI.
   Available at: https://www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html [accessed 24 February 2021]
4. DW.com (2019). China investigates SARS-like virus as dozens struck by pneumonia. DW.com [online].
   Available at: https://www.dw.com/en/china-investigates-sars-like-virus-as-dozens-struck-by-pneumonia/a-51843861 [accessed 24 February 2021]

"Being prepared is all about being able to pick up the weak signals and being ready before something hits you hard. Our example in my case is the pandemic was declared by the WHO on 11 March, and I had my first business continuity committee meeting on the 5th of March, one week before WHO even declared it a pandemic. So as a risk manager, I was watching the situation in China. I alerted my management and I said, "I see this coming and I think we should be ready." We did not have a formal business continuity committee. And I wanted the high-level cross functional-committee and my CEO agreed. We have three vice presidents and seven GMs in the committee.

At that time we did not know what we were going to do, but we had a brainstorm. We figured our biggest issue is going to be the people and the second biggest issue is going to be of course, supply chain. So, when we started to have different types of lockdowns and curfews, I had prepared several different scenarios and sent it to all business units long before it happened. And I had asked what happens if our city is locked down? What happens if our province is locked down? What happens if our overseas shipments are delayed? So, we made sure that we had three to six months of chemicals, essential consumables and anything else critical. And we started working. We have two doctors at the two different sites and they were also part of our committee.

So we had to do lots of things. But we managed absolutely no business impact on any kind of business and we had no financial losses. I believe this is because we were so agile and we adapted so quickly that we managed to weather the storm."

Enterprise Risk Manager, Energy & Utilities, Saudi Arabia

Although some professionals may have been aware of the pandemic prior to the start of 2020, it certainly was not enough of a concern for it to have been considered a major risk to their organizations with a risk score of 2.4 - second from bottom of the risk score index.

The tables were turned this year in dramatic fashion as, non-occupational disease headed to the top of the table with a risk score of 18.6, the highest score ever noted in the annual Horizon Scan report.

Health incident, which languished in 15th position with a score of 3.5 in last year's table of future risks, is in second as a cause of disruption for organizations in the past year. Whilst health incidents will include occupational disease and conditions unrelated to COVID-19, many of those respondents in this year's survey noted it was the secondary effects of COVID-19 which resulted in tangible disruption to their organization during the year. Mental health, for example, had been the cause of extra staff absenteeism over the year as staff felt increasingly isolated from their co-workers. Others witnessed major company restructuring and some had difficulties physically working in their home environments. For organizations who are working on the frontline response, the toll on mental health has been even greater in many circumstances.

"We unfortunately have an increasing number of people accessing the services of our mental health providers for post-traumatic stress and critical incident support. In the emergency services, we are responding to an increased number of road crash incidents possibly due to more people holidaying and driving around the State. There's also been an increased number of suicides and our people are having to respond to those. So in addition to COVID itself impacting us, we are dealing with a higher number of critical incidents and potentially traumatic events, resulting in post-traumatic stress."

Enterprise Risk Manager,
Emergency Services, Australia

"All the health incidents I identified for this survey are primarily due to COVID or one step removed. It's because you're working from home and it's because you're isolated. Obviously, we tracked this, and we asked people to mention if they have contracted COVID so we can look at wellbeing statistics more effectively. Also, one of our key response mechanisms, is wellbeing and mental health. We always ask our managers and leadership to ask how their teams are doing in their team meetings; how are people suffering and things like that. So, the mental health wellbeing aspect is definitely one where it's having an impact on our ability to provide services."

Senior Business Continuity Manager,
Technology, United Kingdom

"I've got a counselling diploma from years back, and previously managed counselling services. So, I'm always very aware of the psycho-social aspects of any of these events. We have an Employee Assistance Program, which is well developed. We regularly remind people about their access to that. That's how we've managed [the mental health side] pretty proactively. It's a normal part of what we do, certainly at the crisis management level. If we have hurricanes, one of the people that we have immediate contact with is our EAP provider to say, 'Okay, there's been this hurricane in three states. Can you tell us what resources you've got?'. They are very proactive and will respond or already have provided information about emergency helplines, evacuation centres and contact for emergency support agencies in state or in country."

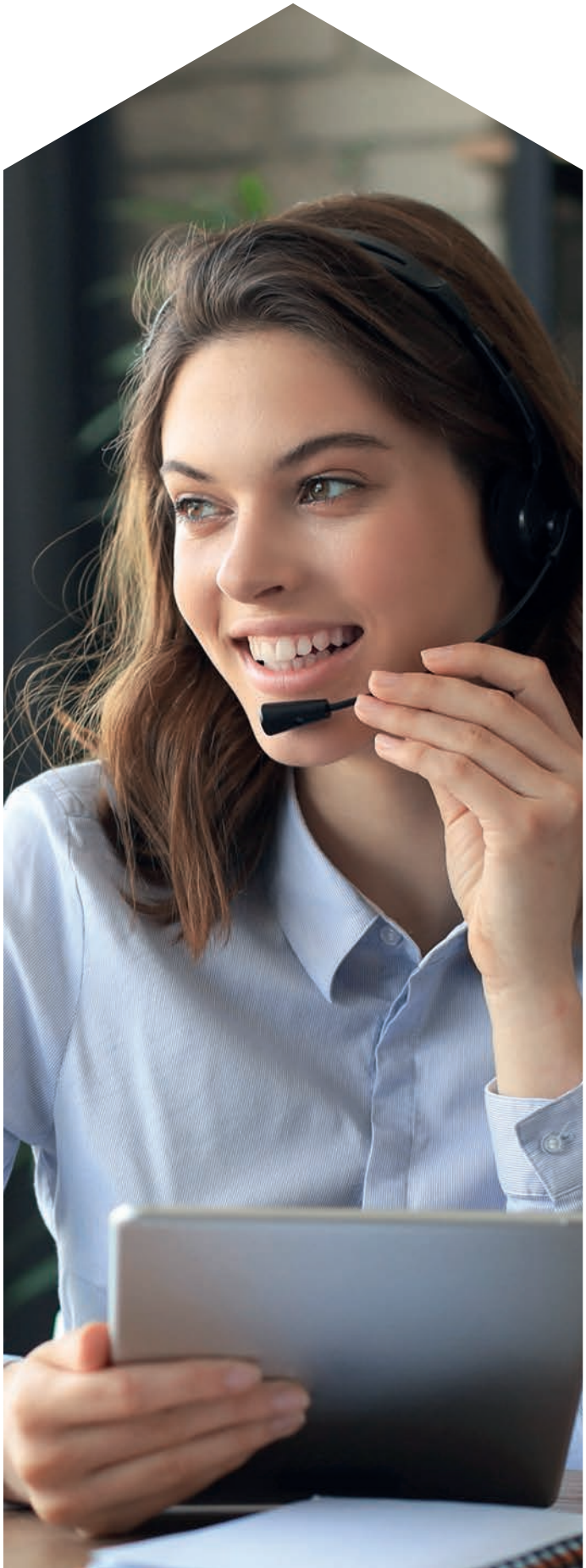
Head of Risk, Healthcare, United States

The longevity of response required for COVID-19 was also something that took many organizations by surprise. Business Continuity plans sometimes only covered the first few days/ weeks of a crisis and did not consider a crisis as long as that experienced with COVID-19.

> **"Our business continuity plans consider the first seven days of a disruption. The prevailing thought was that the crisis management team would within those seven days be able to put strategies in place to either minimize or resolve the event. So, it didn't really consider the impact of a long-term crisis. We did consider what would happen if 30% of people working on critical functions were absent, but not the whole bank; everyone working from home. If we had considered this first, we wouldn't have needed to test working remotely on the fly two days before the country was locked down."**
>
> Business Continuity Manager,
> Financial Services, New Zealand

Safety incidents also remained high this year, despite many staff being away from company sites. Interviewees reported that COVID-19 had prompted their organizations to better record health and safety incidents this year, whilst others said that incidents had occurred on site as a result of staff having to carry out work they had not been properly trained for due to staff absence and/or furlough. Other organizations noted an elevated risk when staff switched to remote working environments with equipment not being fit for purpose.

Supply chains were also one of the headline impacts of COVID-19 with the impacts of this being produced in Horizon Scan's sister report, Supply Chain Resilience 2020. Critical suppliers were unable to meet contractual requirements due to logistics issues, manufacturing sites being closed as a result of infection outbreaks and problems occurring deep in tier 2 suppliers and beyond. Although as COVID-19 progressed some initial problems were resolved, supply chain issues continue today with a global container shortage causing substantial delays and prohibitive cost rises to many organizations[5].



5. Tan, W (2021). An 'aggressive' fight over containers is causing shipping costs to rocket by 300%. CNBC [online]. Available at: https://www.cnbc.com/2021/01/22/shipping-container-shortage-iscausing-shipping-costs-to-rise.html [accessed 11 March 2021]

"There was a difficulty in getting some routes arranged, although we managed to get round this. For example, if we normally flew from Hong Kong to London, there may not be a direct flight available and they would have been re-directed to a different available route. So, from a distribution point of view, we had everything sorted out. However, from a production perspective, getting goods from the Netherlands to other parts of Europe had problems because when the truck drivers would be traveling through different countries they would be stopped at the border. But again, those were initial teething issues, most got ironed out as soon as we could give them the right information about goods being essential and we had licenses, so we did manage to get round it."

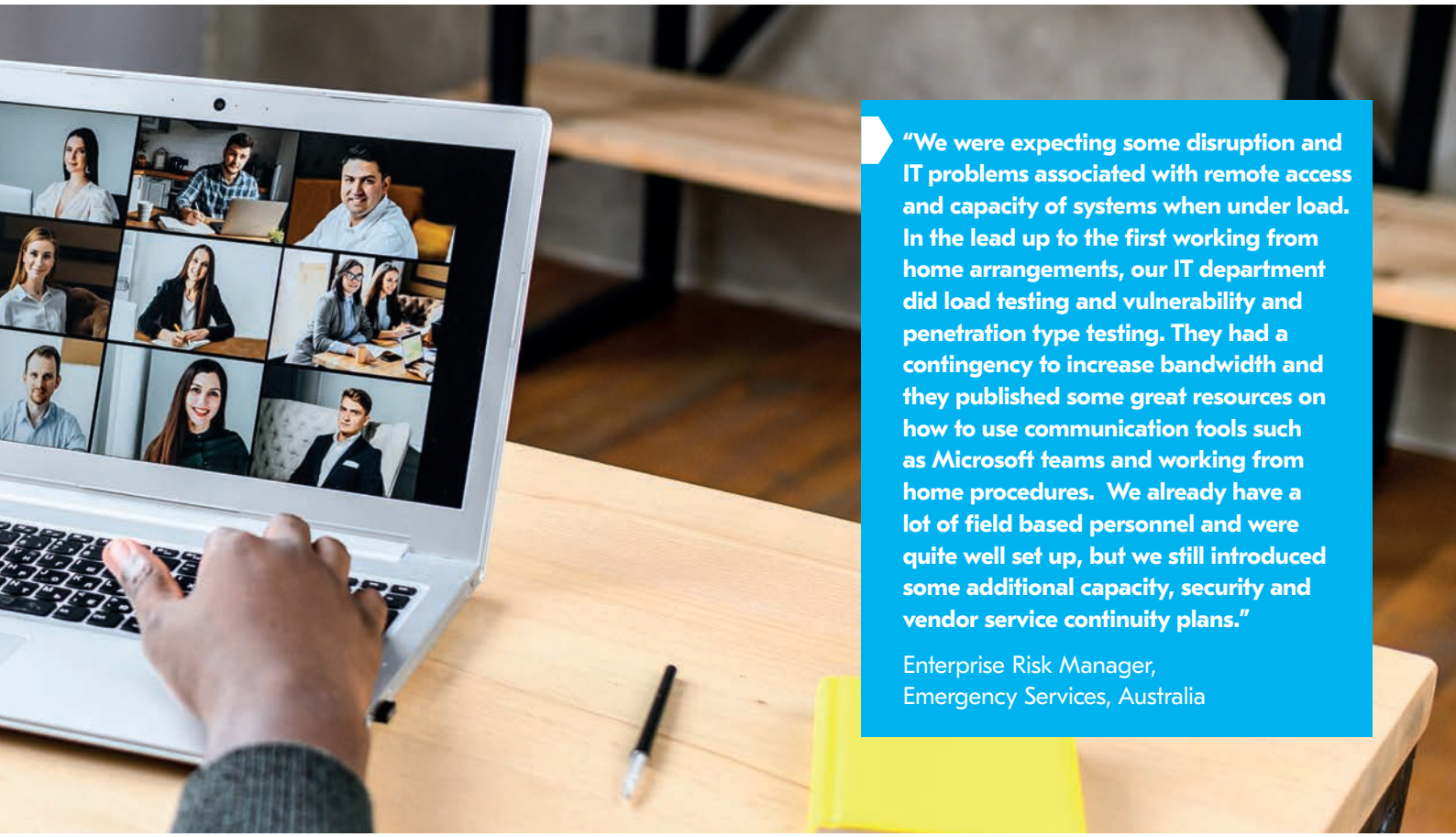
Head of Business Continuity, Electronics, United Kingdom

"Everyone is experiencing global distribution logistics challenges. Normal contingency and recovery plan options are just not available now due to shortages of shipping containers, trucks, drivers or constraints at ports. There is no way to influence this global dynamic, not even at a regional level. Many companies' upside potential is being affected by these challenges."

Business Continuity Manager, Consumer Goods, United States

Nevertheless, despite the overriding disruption caused by COVID-19, organizations still experienced enough IT and telecom outages for it to remain in fourth place in the list of disruptions for 2020 with a risk score of 15.8 — 2.8 higher than in the 2020 report. The increased use of technology because of changing working practices led to an increased number of disruptions this year. The use of collaborative software for communication purposes through tools such as Zoom or Microsoft Teams, for example, helped to drive global internet traffic up by 35% during 2020. Even in Africa, where technology uptake is typically lower than the rest of the world, usage increased by 46%[6]. At the period when most organizations switched to remote working — March 2020 — ThousandEyes reported a 63% increase in global internet disruptions compared to January[7]. This meant IT departments had to ensure their networks could cope with the extra capacity and ensure systems were working correctly for staff to work remotely.

Whilst it could be argued that these disruptions were caused by external, often global, outages, it does emphasise the importance of considering how an overnight shift to increased technology usage should be addressed in future planning. Extreme weather events, for example, might cause similar volumes of people to move to remote working and could cause overloading of local networks.



"We were expecting some disruption and IT problems associated with remote access and capacity of systems when under load. In the lead up to the first working from home arrangements, our IT department did load testing and vulnerability and penetration type testing. They had a contingency to increase bandwidth and they published some great resources on how to use communication tools such as Microsoft teams and working from home procedures. We already have a lot of field based personnel and were quite well set up, but we still introduced some additional capacity, security and vendor service continuity plans."

Enterprise Risk Manager,
Emergency Services, Australia

6. Brodsky, P (2020). Internet Traffic and Capacity in Covid-Adjusted Terms. TeleGeography [online]. Available at: https://blog.telegeography.com/internet-traffic-and-capacity-in-covid-adjusted-terms [accessed 24 February 2021]
7. ThousandEyes (2020). Internet Performance Report: COVID-19 Impact Edition. ThousandEyes [online]. Available at: https://marketo-web.thousandeyes.com/rs/thousandeyes/images/ThousandEyes-Internet-Performance-2020-Final.pdf [accessed 24 February 2021]

Telecommunication networks were also hit by increased usage: the UK's EE, Three and O2 operators reported a major outage in March 2020 due to a surge in demand[8] and Australia's Telstra reported similar issues at the same time[9].

Distributed Denial-of-Service (DDoS) attacks were also rife in 2020, with criminals exploiting the fact that organizations had concentrated IT resources on implementing remote working processes and/or had reduced levels of IT staff on site because of the pandemic. This meant some IT departments were overstretched and systems were more vulnerable to attack. In May 2020, Netscout observed 929,000 DDoS attacks — the largest number ever seen in a month — and attacks between March and June 2020 increased by 25% when compared with the three years prior[10]. Disruption did start to wane throughout the year however and, by May 2020, the Body of European Regulators for Electronic Communications reported that the initial problems had now stabilised[11].

Extreme weather in itself was still a major cause of disruption in 2020, ranking at sixth place on this year's risk index with a score of 12.3. The world saw more than its fair share of weather events in 2020: Sydney, for example, recorded its highest ever temperature (48.9°C) and bushfires in the country destroyed 10 million hectares to create the largest ever recorded smoke cloud (620 miles wide/21 miles high). California also suffered a record year for wildfires with over 1.6m hectares destroyed and super-cyclone Amphan was the strongest cyclone to hit the Bay of Bengal this century and was also the costliest on record with losses in India alone put at $14bn. More recently, the snowstorms which covered 71% of America in February 2021 led to huge levels of disruption to businesses. In Texas, where snowstorms are rare, an early estimate of the cost of disruption has been put at $50m[12]. In fact, the number of weather-related disruptions during the year has caused many organizations to consider climate risk in their mid- to long-term planning for the first time.

"Environmental change is the other thing for us. Historically, we are an energy company founded in an industrial economy, and our roots are firmly embedded in coal. We generate a lot of energy from it, and it occupies a significant share of the generating capacity, both for us and for our parent company. This means that decarbonizing power generation is having a big impact on the company going forward. We are, however, working to mitigate this with a relatively rapid shift towards low carbon forms of energy generation, through both acquisition and collaborative projects with other organizations. Other problems as well arise from environmental factors; we get a lot of organized activist action, which can cause a lot of damage particularly from a PR perspective."

IT Risk Manager, Energy & Utilities, United Kingdom

"After COVID, I think one of the major risks is climate change. For our business, it's a regulatory condition as well that we have to say how we're managing climate change and how we're supporting the environment. And that takes up a lot of effort because of our global presence. And I'd have to say that as soon as people start returning to normal working life in the city in whatever shape or form that is, the terrorist threat for me will reappear. "

Group Business Continuity Manager, Financial Services, United Kingdom

8. Martin, A (2020). Coronavirus: O2 network outage as people work from home. Sky News [online]. Available at: https://news.sky.com/story/coronavirus-o2-network-goes-down-as-people-work-from-home-11958924 [accessed 24 February 2021].
9. Fookes, T & Condon, M (2020). Mobile phone network strain caused by coronavirus isolation causing dropouts. ABC News [online]. Available at: https://www.abc.net.au/news/2020-03-25/mobile-phone-network-congestion-blamed-on-coronavirus-calls/12087856 [accessed 24 February 2021]
10. Vijajan, J (2020). DDoS Attacks Spiked, Became More Complex in 2020. DARKReading [online]. Available at: https://www.darkreading.com/attacks-breaches/ddos-attacks-spiked-became-more-complex-in-2020/d/d-id/1339814 [accessed 24 February 2021]
11. BEREC (2020). Overview of the Member State experiences related to the regulatory and other measures in light of the COVID-19 crisis. Body of European Regulators for Electronic Communications [online]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71426 [accessed 24 February 2021]
12. BBC, The (2021). Texas weather: Deaths mount as winter storm leaves millions without power. BBC [online]. Available at: https://www.bbc.co.uk/news/world-us-canada-56095479 [accessed 24 February 2021]

Regulatory changes has also risen in the list of disruptions during the past year, climbing to 9th position from 15th in the previous report. Respondents from the EMEA region commented that regulatory changes were primarily focused around Britain's exit from the European Union, with hastily introduced regulations related to COVID-19 or Governmental changes causing disruption globally. One interviewee reported that the good response from their Government had actually helped to elicit a good response in their organization and praised the Government for doing so.

"I'd say the government of Saudi Arabia has been in the top five countries in terms of controlling and responding to this pandemic. Almost on a daily basis we were getting new directives, news about curfews as well as all the new regulations coming in, such as social distancing. This really helped us in our response."

Enterprise Risk Manager, Energy & Utilities, Saudi Arabia

BSI's Supply Chain Intelligence reveals new regulations adopted around the world will have a direct, lasting impact on global supply chains. For example, proposed EU regulations are meant to hold firms to account for environment and human rights abuses in their supply chain. New legislations in North America and Europe are designed to curb illegal deforestation in supply chains. There are fast-approaching deadlines in the US to begin enforcement of increased security screening of cargo shipments and exports.

Each of these regulatory changes - and many more- will add layers of complexity to operations. Also, non-compliance in these evolving conditions will increase the potential for continuity disruption.

Although its position has only climbed a single place in this year's risk index, the introduction of new technology was highlighted as a disruption which came to the fore this year. Many organizations switched to new tools and technology to help workers adapt to a remote working environment, whilst others invested in emergency communications tools to more efficiently alert staff who were out of the office. Other organizations invested in new technology to better understand the risk landscape and their supplier network. Although positive steps in the long term, the short-term introduction of new technologies did lead to some disruption, particularly as most training for new products had to be carried out in a remote environment.

> **"I had such a high frequency [of disruptions due to new technology] because of the shift to working remotely. Everyone had Teams installed on their laptops but nobody got trained in how to use it. Also different teams had different products to use and needed a lot of effort from IT to get people fully comfortable with those. There were also politicians who were elected to pass legislation and hold the government to account which helped to focus resources on stability of our remote participation tools."**
>
> Business Continuity Manager, Public Sector, United Kingdom

One of the positive trends to have come out of this year's risk analysis is the decline of "Lone attacker/ active shooter incident" to second from bottom in this year's table, down from 12th position in 2020. With most workers not being tied to a physical workplace in 2020, the chances of a premises-based attack were significantly reduced. However, in the same way that "pandemic" was not considered a risk in 2020 by many responding to last year's survey, resilience professionals must ensure that risks such as workplace violence are not ignored in this year's planning cycle.

Ranking		Frequency	Impact	Risk Index
1	Non-occupational disease (e.g. pandemic)	5.9	3.2	18.6
2	Health incident (occupational disease, reportable occupational disease, stress/ mental health, increased sickness absence)	7.8	2.3	18.2
3	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	7.5	2.2	16.1
4	IT and telecom outage	6.0	2.6	15.8
5	Cyber attack & data breach	7.3	2.1	15.3
6	Extreme weather events (e.g. floods, storms, freeze, etc.)	5.2	2.4	12.3
7	Lack of talent/key skills	5.3	2.3	12.1
8	Supply chain disruption	5.1	2.3	12.0
9	Regulatory changes	5.3	2.2	11.7
10	Interruption to utility supply	5.0	2.3	11.3
11	Political violence/civil unrest	5.1	1.8	9.4
12	Natural resources shortage	5.7	1.6	9.3
13	Introduction of new technology (IoT, AI, Big data)	4.3	2.1	9.0
14	Exchange rate volatility	4.6	1.9	8.8
15	Critical infrastructure failure	4.3	2.1	8.7
16	Product safety recall	5.2	1.7	8.7
17	Enforcement by regulator	4.2	2.0	8.3
18	Political change	4.0	2.1	8.1
19	Natural disasters (earthquakes, tsunamis, etc.)	4.2	1.9	7.8
20	Higher cost of borrowing	4.3	1.7	7.3
21	Lone attacker/active shooter incident	3.4	1.6	5.7
22	Energy price shock	3.2	1.7	5.4

Figure 1. Risk and Threat Assessment: Past 12 Months

The risk score is calculated by multiplying the frequency and impact numbers. Numbers have been rounded to the nearest tenth in the report, so may differ slightly from the calculated figures.

Risk and threat assessment: past twelve months

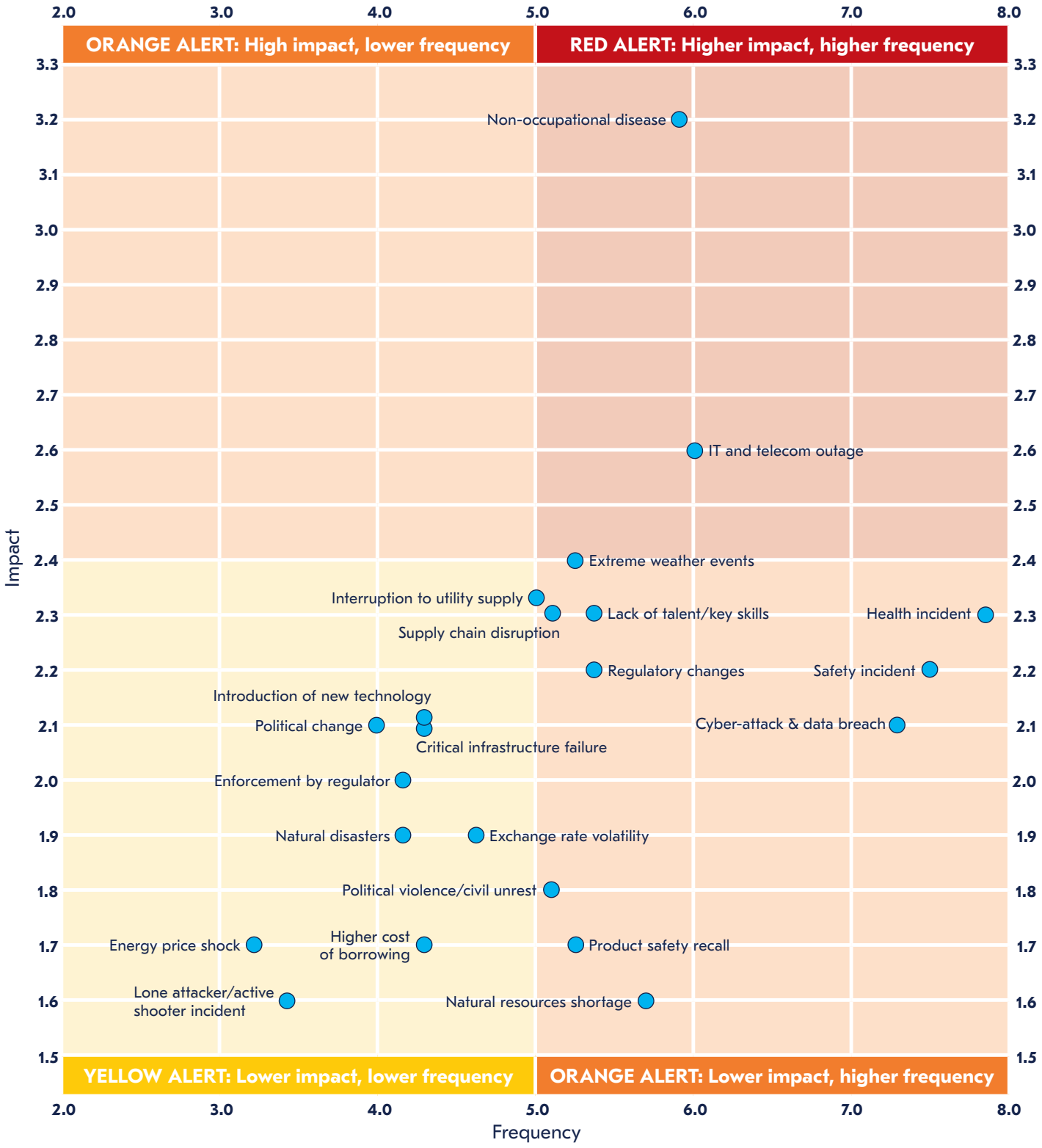
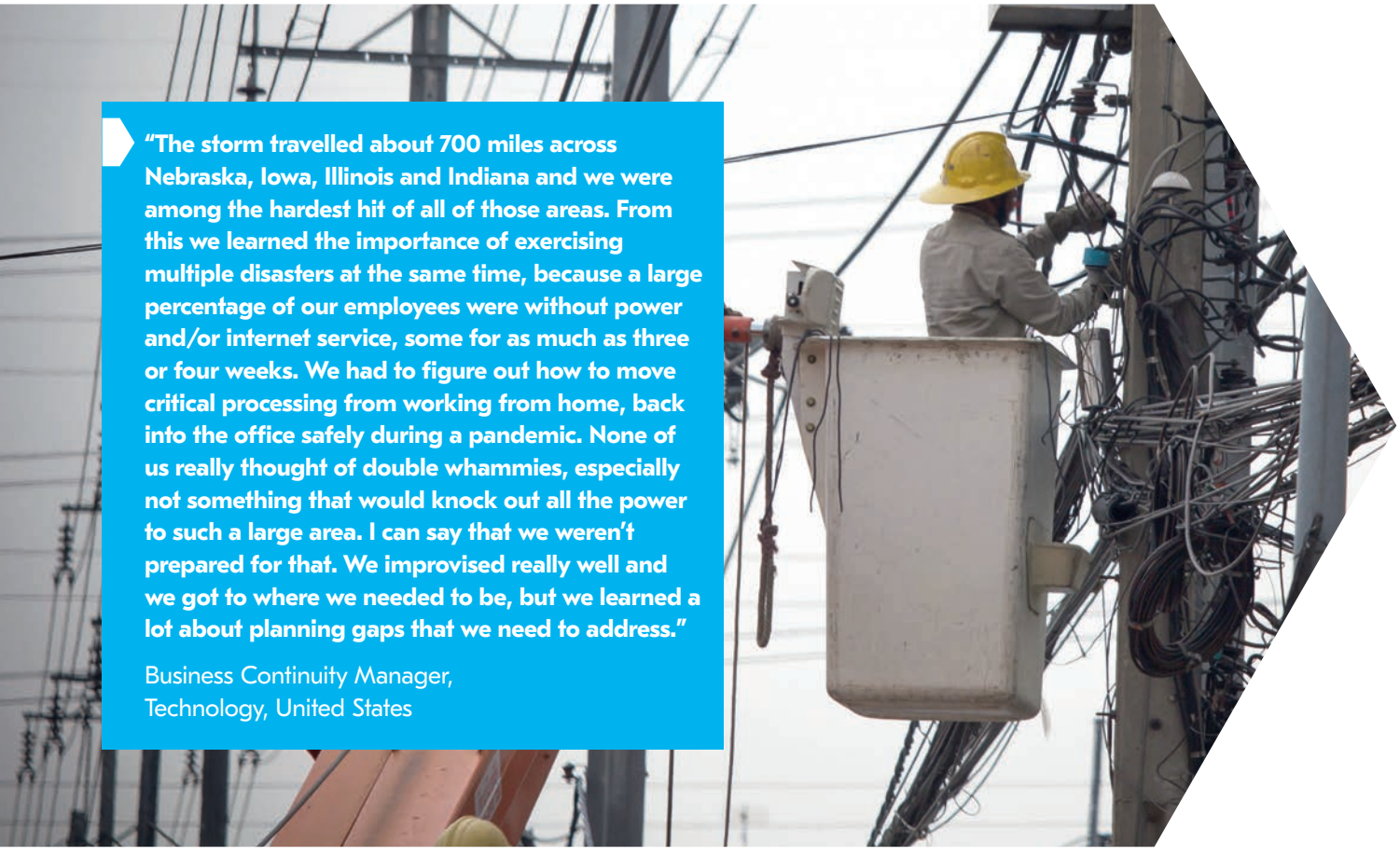


Figure 2. Risk and Threat Assessment: Past 12 Months

When respondents were asked to consider their greatest disruption in 2020, most understandably responded with "communicable disease". However, what is also surprising is that a third (33.0%) of organizations did not consider it to be their greatest disruption. Many office-based organizations reported that COVID-19 had very little to no impact at all with staff able to revert to remote working models overnight. For such organizations, the primary problems were IT and telecom outages, primarily caused by wider network issues. Therefore, whilst system outages may have been the cause of the disruption, the outage was blamed by many as being a secondary disruption of COVID-19. This shows that even when faced with a global crisis, other major disruptions can — and will — continue to occur. Being prepared for multiple events occurring at the same time is something all organizations should consider. One interviewee explained how their area in the United States was hit by a storm which caused a power outage for the whole County — whilst everyone was working from home. The only solution was to get workers back into the office in a COVID-safe environment.

"One of the risks we had focused on was not only a COVID outbreak, but managing a COVID outbreak concurrently with another emergency such as a bush fire. What we hadn't considered was bush fires, floods, and a COVID outbreak. So our biggest challenge was managing our available resources during that time. When we had to get assistance from outside of the regions in lockdown, we used a number of segregation strategies to keep those people separate, in sort of bubbles. We had to manage these different groups and teams of people using different measures. We did have really good plans though and I'm proud of how they were used."

Enterprise Risk Manager,
Emergency Services, Australia



"The storm travelled about 700 miles across Nebraska, Iowa, Illinois and Indiana and we were among the hardest hit of all of those areas. From this we learned the importance of exercising multiple disasters at the same time, because a large percentage of our employees were without power and/or internet service, some for as much as three or four weeks. We had to figure out how to move critical processing from working from home, back into the office safely during a pandemic. None of us really thought of double whammies, especially not something that would knock out all the power to such a large area. I can say that we weren't prepared for that. We improvised really well and we got to where we needed to be, but we learned a lot about planning gaps that we need to address."

Business Continuity Manager,
Technology, United States

Which event was the cause of your most major disruption in the past year?

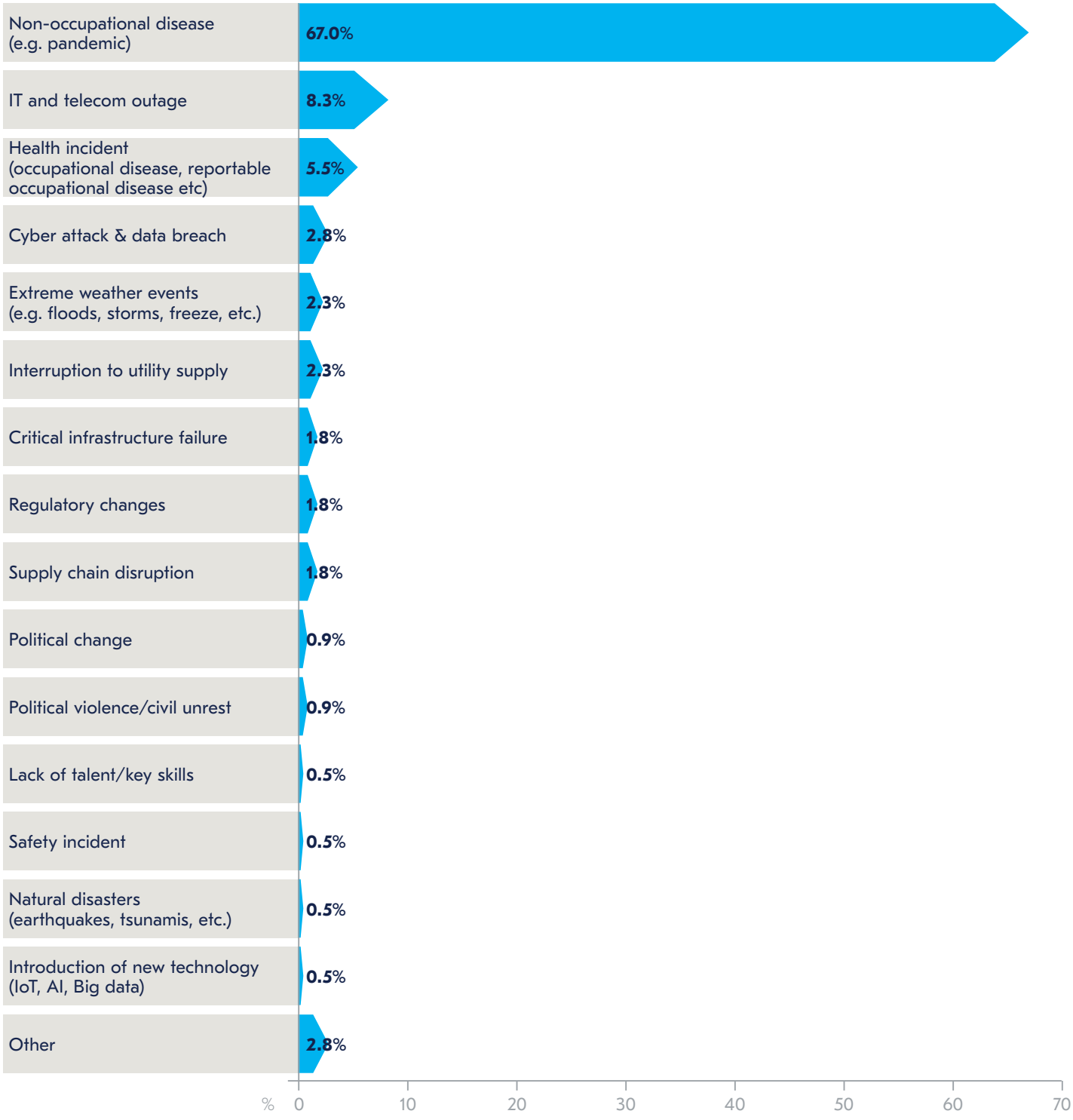


Figure 3. Which event was the cause of your most major disruption in the past year

Risk and threat assessment: next twelve months

Risk and threat assessment: next twelve months

- Organizations had the starkest reminder of the importance of being prepared for the unexpected in 2020 and are better at considering grey rhino or black swan events in their future risk landscapes.
- Disconnects still exist in terms of what has happened and what will happen with professionals' concerns diverted to the risks they feel they have little control over. Safety incidents placed third on the list of disruptions for the past year, yet places 15th in the risk index for the next twelve months.
- Political change and political risks/violence have both risen sharply in the risk index for the next twelve months. Protests in the wake of the death of George Floyd, global riots relating to COVID-19, politically charged riots surrounding the US presidential election as well as large demonstrations in France, Chile, Ecuador and Hong Kong have all led to increased concern around the topic for 2021.
- IT disruptions continue to be a concern as organizations seek technological change to help address new working practices.

The second part of the risk and threat assessment looks at the disruptions which are top of mind for professionals over the next year. An individual risk score is calculated for each incident based on perceived likelihood and the impact of that incident occurring.

Each year, this report notes a disconnect between those incidents that have occurred within organizations versus those which they perceive will occur. Respondents are typically concerned about incidents which they feel unable to control (such as natural disasters or, in this year's report, non-occupational disease) and are less concerned about failures which are typically caused by human or company error (i.e. those where they feel they do have more control). Health incidents, for example, were second in the list for incidents which occurred over the last year, whereas the category falls to eighth place in the risk index for the following year. Safety incidents has an even greater fall, tumbling to 15th position in the risk index for the next twelve months, even though it took third place for past disruptions. The fact that there is so much discrepancy year-on-year with organizations overlooking these major causes of disruption indicates that risk analysis could be performed better in organizations. It is good practice for those working on horizon scanning to not just take into account the broader risk landscape for the future, but also combine it with an exercise at scanning the patterns of disruption in their own organization over the past year.

This importance of "being prepared for the unexpected" has been discussed every year in the Horizon Scan report. This year, however, COVID-19 has proved to be the ultimate lesson in preparing for events dubbed "grey rhino" events (events which are highly probable, have a high impact but are often overlooked). Last year's Horizon Scan report placed "non-occupational disease" as second from last in the list of concerns whereas it turned out to be the cause of greater disruption than many organizations had experienced in their history. Although business continuity departments in many organizations did have the necessary plans made and were able to invoke them quickly and efficiently, many found plans had not been updated and were certainly not fit for accounting for the intricacies associated with COVID-19 (e.g. pandemic plans considering mass staff absences, but not considering mass remote working).

"Over the years we've been doing a lot of testing on our business continuity plans. Especially around remote working and the loss of the building. Which in theory is what we had during COVID. We couldn't go into our offices. The vast majority of our staff would have their own work laptops and everyone's very used to using remote working technology. So when we were testing remote working, we were always getting great results from investment in this technology. The dependency on an office wasn't there, it wasn't a requirement. So we had very little impact in that respect."

Head of Business Continuity Management, Real Estate, Asia

"In December 2019 we conducted a pandemic exercise based on a flu-like virus so we were very wary of what was happening abroad in early 2020. In terms of creating a plan to an actual pandemic we had a good start, but we weren't prepared for a national lockdown. We were prepared for trains not running, for shops to be closed, and for people to be ill. But we weren't prepared for how long we would not be going to work."

Business Continuity Manager, Public Sector, United Kingdom

"IT was well prepared for COVID-19 and remote working. IT has been preparing the past few years to be more flexible in how we worked and where we worked. And so that played very well into what we needed to do. Some other parts of the business were not quite so prepared. They had not been pushed to make some of the changes, like working from home. So it took them 30 or 45 days to really make that transition comfortably. Was the IT organization ready to support that? Not entirely. We had to make some changes in the products and services that we were offering. So, while IT was able to transition to working from home and able to continue supporting the business, we needed to tweak some things which took us 45 days."

Business Continuity Manager, Technology, United States

Other organizations are already considering changing how they plan for crises as a result of the learnings made during COVID-19.

"I'm always of the opinion that we should be building frameworks that are hazard agnostic. So not delving too deep into specific threats but building a program that is malleable. There is a need to get across to senior leadership the concept that every crisis event is going to be unique. Even if you've got a pandemic plan, that is not going to 100% fit the disruption."

Business Continuity Manager, Financial Services, New Zealand

"The risk profile of the world has changed, and we're aware of that. In terms of looking forward, some of the countries we operate in we would consider kidnap and criminal risk is going to be higher once business starts operating again. There are changes in terms of some of the criminal activities in some of the countries we operate in that have been affected by COVID. I was on a briefing two days ago looking at the situation in Mexico where they're thinking that there will be more overt criminal non-drug cartel related activity now going on. We see quite a lot in the environment in which we work as risks and heightened risks. Most of these things you can attribute to COVID in one way or another because the world has changed and therefore risk factors have changed. And some of the factors that lead to these activities have changed."

Head of Risk, Healthcare, United States

The difference this year, however, is organizations are learning from the experiences of COVID-19 and are now giving grey rhino and black swan events more consideration in their planning. Interviewees reported plans were now being rewritten in earnest, with more attention being paid to risks which had previously been ignored as they were deemed very unlikely to occur (e.g. lone attacker). The most astute professionals are already viewing COVID-19 as an exercise to improve internal processes rather than wait for the traditional post-incident review which, in the case of COVID-19, is likely to be many months away.

"We've also undertaken a very large, enterprise wide, lessons learned project following COVID. We polled all of the business continuity and crisis management teams on various areas of focus. We touched on business continuity and local response; crisis management and health and safety. Then we also looked at HR and data privacy. We also touched on comms and how they felt the corporate communications worked to inform staff. That gave great feedback and we've been able to take some of those forward to improve our processes in 2021."

Head of Business Continuity Management, Real Estate, Asia

Other interviewees discussed that they were now taking a longer term look at risk planning, with the impact of climate change now being discussed from a risk and resilience perspective rather than one which was traditionally paid lip service in the corporate social responsibility pages at the end of Annual Reports. Indeed, industry experts are discussing how COVID-19 should serve as a lesson in demonstrating how destabilising risks from outside the financial system can quickly cascade through markets and economies. In a piece by Bob Bailey, Director of Climate Resilience at Marsh & McLennan Advance, he has highlighted how he believes the next major incident is likely to come from an event he calls a "green swan" event . A view subscribed to by many other Resilience professionals evidenced by interviews carried out for this report.

> **"I think there is an increased focus on risk and using risk tools and resources to help prioritise activities. Recent discussions on emerging risks include hydrocarbon installations, battery energy storage systems, and autonomous vehicles and how, for example, we would safely respond to a significant battery fire. I feel people are more proactive when it comes to using risk to inform decision making, and if anything COVID has actually helped raised awareness of using risk in that respect."**
>
> Enterprise Risk Manager, Emergency Services, Australia

Extreme weather events remain a top-of-mind concern for many resilience professionals during 2021 and, as highlighted in the previous section, such events are becoming more widespread and more extreme. The overall risk score (4.8) is slightly lower than that in the 2019 report (4.9), but professionals consider the likelihood of such an event happening as higher. Indeed, there are parts of the world where concern for extreme weather events is higher than the rest of the world. *BCI's Emergency Communication Report 2020* showed that emergency communications plans were activated by American organizations more in 2020 for extreme weather events than for COVID-19 related communications. Furthermore, the extreme cold weather encountered in the central United States in February 2021 is likely to have elevated concerns for the coming year. With temperatures reaching 30-year lows of -18°C in Texas, organizations have been hit with challenges they have not encountered in recent history. Had the survey for this report closed at the end of February, extreme weather events may have been allocated a higher risk score.

IT and telecom outage placed third in this year's risk index for the next twelve months. In previous years, the prevailing concerns have been around network outages and system failures. Although these remain a point of concern to resilience professionals, the latency issues experienced during the past year coupled with the introduction of new technologies add additional vulnerabilities to the IT landscape.

The most notable change from last year's Horizon Scan report is the risk of political change and political violence/civil unrest with both attaining higher risk scores than last year. This rise in political risk has also been noted in other risk indices in 2021: the Allianz Risk Barometer 2021 noted that political risks and violence had returned to the top 10 in their index for the first time since 2018. Indeed, 2020 saw a year of heavy political violence. The death of George Floyd led to racially charged protests globally, some of which were violent. The US also experienced riotous protests at the US Capitol building because of the US Presidential Election. According to Allianz, protests in France led to losses of $90m, in Hong Kong $77m, Chile $2bn and Ecuador $821m[14]. Throughout the world, anti-lockdown riots have also been causing local disruption for many organizations.

13. Bailey, R (2021). Planning for the Unexpected: COVID-19 Is a Dry Run for Climate Catastrophes. BrinkNews [online]. Available at: https://www.brinknews.com/green-swan-climate-events-how-to-plan-for-the-unexpected-coronavirus-risk-environment/ [accessed 24 February 2021]
14. Allianz (2021). Allianz Risk Barometer 2021 - Political risks and violence. Allianz [online]. Available at: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2021-political-risks.html [accessed 24 February 2021]

"What we're starting to see is a rise in right-wing extremism. I think COVID is going to exacerbate this subject further. Especially if populations perceive that their governments have not been able to achieve as much as they expected regarding COVID response. We saw this a few years back in Europe with some right-wing organizations pushing that hate message to favour their aims. So, extremism, which could have a knock-on impact to business, is an area we're focusing on at the moment."

Head of Business Continuity Management, Real Estate, Asia

The concerns surrounding COVID-19 and the multiple examples of civil unrest this year show how incidents experienced during the previous year impacts risk planning in the year ahead. What is notable, however, is that the experience with COVID-19 has prompted many organizations to take a broader view of the risk landscape and consider risks which have recently waned in occurrence but are still likely to happen. Active shooter, for example, fell to second from last in the risk index for 2020, but moves to 16th position with a risk score of 3.8 (2019: 3.6) when organizations consider their risks for 2021.

Widespread and large-scale man-made disruptive events initially decreased in the first half of 2020 due to lockdown measures. Despite this decrease in activity during the first months of the pandemic, protests and man-made disruptions were organized and sustained to historic numbers in 2020.

Even if the protests did not directly have an impact on business operations, these demonstrations have had impacts on organizations. At a minimum, they have had to divert internal resources to monitor events as well as preparing for the possibility of implementing mitigation measures to ensure the continuity of operations or safety of personnel.

These issues highlight the need to not discount events based on the initial assumption that there is no direct impact to the organization, as there is a chance for secondary or tertiary impacts to occur that will require a response by some other facet of the business.

BSI Supply Chain Intelligence

"There is now a more widely perceived value in looking at what is happening in the national space [as a result of COVID-19]. What do the wider risks mean for us? What affects me being in a particular institute or organization, and planning for those? We don't have anyone looking at that formally yet. So while we are looking at our resilience approach, we never had formal horizon scanning. So that's a gap and that's something that we'll be looking to take on; lifting your head up and being objective about the extra risks. It's not about the UK, it's about what other similar organizations are experiencing across the world. We want to try and get ahead of the game, actually help people think through what's on the horizon, identify a gap, try to articulate the risk, in terms of different geographies. Looking back to February 2020 and seeing what can be leveraged and what can be discarded rather than doing rushed lessons-learned or a rushed evaluation of IT; this isn't necessarily about making things cheaper but working out what to invest in."

Business Continuity Manager, Public Sector, United Kingdom

Elsewhere, there is little change in the overall risk landscape for the following year. Cyber-attacks and data breaches are ranked in second place this year behind non-occupational disease. Interviewees reported a more elevated concern about cyber incidents over the coming year, and the risk score has risen slightly to 6.6 (2019: 6.4) which reflects this. Cyber incidents increased over the course of 2020 as attackers preyed on workers' elevated concerns around COVID-19 through carefully orchestrated phishing attacks. In the first quarter of 2020, global phishing attacks increased by 600%[15]. In May 2020 in the UK, Her Majesty's Revenue & Customs (HMRC)'s released data to show that 5,152 phishing scams reported by the public, up 337% on March when lockdowns first came into place[16]. CheckPoint Research notes in November 2020, there were 1,062 "potentially malicious" domains registered relating to vaccines: more than the previous three months put together[17]. Google meanwhile reported in April last year it was blocking 240 million COVID-themed spam emails every day and 18 million malware and phishing emails[18]. Although most professionals interviewed for this report had a high level of confidence within their IT departments to thwart attacks, many reported they were going to step-up security arrangements during 2021.

15. Sjouwerman, S (2020). Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600%. KnowB4 [online]. Available at: https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600 [accessed 24 February 2021].
16. Coker, J (2020). HMRC Investigating Over 10,000 COVID-Related Phishing Scams. Infosecurity Magazine [online]. Available at: https://www.infosecurity-magazine.com/news/hmrc-investigating-covid-related/ [last accessed 15 January 2021].
17. Scroxton, A (2020). Surge in Covid-19 vaccine phishing scams reported. Computer Weekly [online]. Available at: https://www.computerweekly.com/news/252493523/Surge-in-Covid-19-vaccine-phishing-scams-reported [last accessed 15 January 2021].
18. Muncaster, P (2020). Google: We Block 240 Million Daily #COVID19 Spam Messages. Infosecurity Magazine [online]. Available at: https://www.infosecurity-magazine.com/news/google-block-240-million/ [accessed 24 February 2021]

"But the cyber threat environment is big for us this year for two primary reasons. The primary cause of this is geopolitical, Canada finds itself caught in the middle of this ongoing superpower rivalry and with Canadian cyber defence infrastructure being fairly weak compared to our neighbours to the South it makes us an obvious and easy target for state backed cyber efforts to apply pressure geopolitically. Additionally, given the huge Chinese cultural influence in Vancouver, about 45% of the population are ethically Chinese heritage there is additional potential to mobilise elements of the community into physical activism and civil unrest as we have already seen manifested in protest. Secondly, Canada has seen a marked uptick in major cyberattacks last year with a number of high-profile examples over the last 12 months. This combined with the surge in COVID-19 homeworking and the technical exposures this opens up has left us feeling a lot more vulnerable to exploitation and attack".

Business Continuity Manager, Automotive, Canada

"Basically we've had to shut off SolarWinds because of that potential breach. We weren't breached, and all through last year we were adding more and more cyber security scanning equipment. We've really increased the footprint on the defences, on cyber security, and that's going to continue. For our tabletop exercising this year, we're going to do a special one just with our security team for responding to a cyber-attack, with the security team and the IT team. How do we recover from this? That's become first and foremost the heaviest deal."

Director of IT & Resiliency,
Financial Services, United States

The other area of note where practitioners continue to have an elevated interest in 2021 is in supply chain. With supply chains dramatically affected by the pandemic, practitioners believe that disruptions will continue to be felt in 2021, and potentially with the added issue of boycotting of supply chains and conflict.

	Ranking	Likelihood	Impact	Risk Index
1	Non-occupational disease (e.g. pandemic)	3.9	2.3	9.0
2	Cyber attack & data breach	3.1	2.1	6.6
3	IT and telecom outage	2.9	1.8	5.2
4	Regulatory changes	2.8	1.8	5.0
5	Extreme weather events (e.g. floods, storms, freeze, etc.)	3.0	1.6	4.8
6	Critical infrastructure failure	2.4	2.0	4.8
7	Supply chain disruption	2.5	1.8	4.5
8	Health incident (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	2.8	1.6	4.5
9	Lack of talent/key skills	2.6	1.7	4.4
10	Natural disasters (earthquakes, tsunamis, etc.)	2.1	2.1	4.4
11	Introduction of new technology (IoT, AI, Big data)	2.7	1.6	4.3
12	Interruption to utility supply	2.5	1.6	4.0
13	Political change	2.5	1.6	4.0
14	Enforcement by regulator	2.3	1.7	3.9
15	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	2.4	1.6	3.8
16	Lone attacker/active shooter incident	1.8	2.1	3.8
17	Political violence/civil unrest	2.2	1.6	3.5
18	Exchange rate volatility	2.4	1.4	3.4
19	Higher cost of borrowing	2.1	1.5	3.2
20	Energy price shock	2.0	1.4	2.8
21	Natural resources shortage	1.8	1.5	2.7
22	Product safety recall	1.5	1.5	2.3

Figure 4. Risk and threat assessment: next twelve months

The risk score is calculated by multiplying the likelihood and impact numbers. Numbers have been rounded to the nearest tenth in the report, so may differ slightly from the calculated figures.

Risk and threat assessment: next twelve months

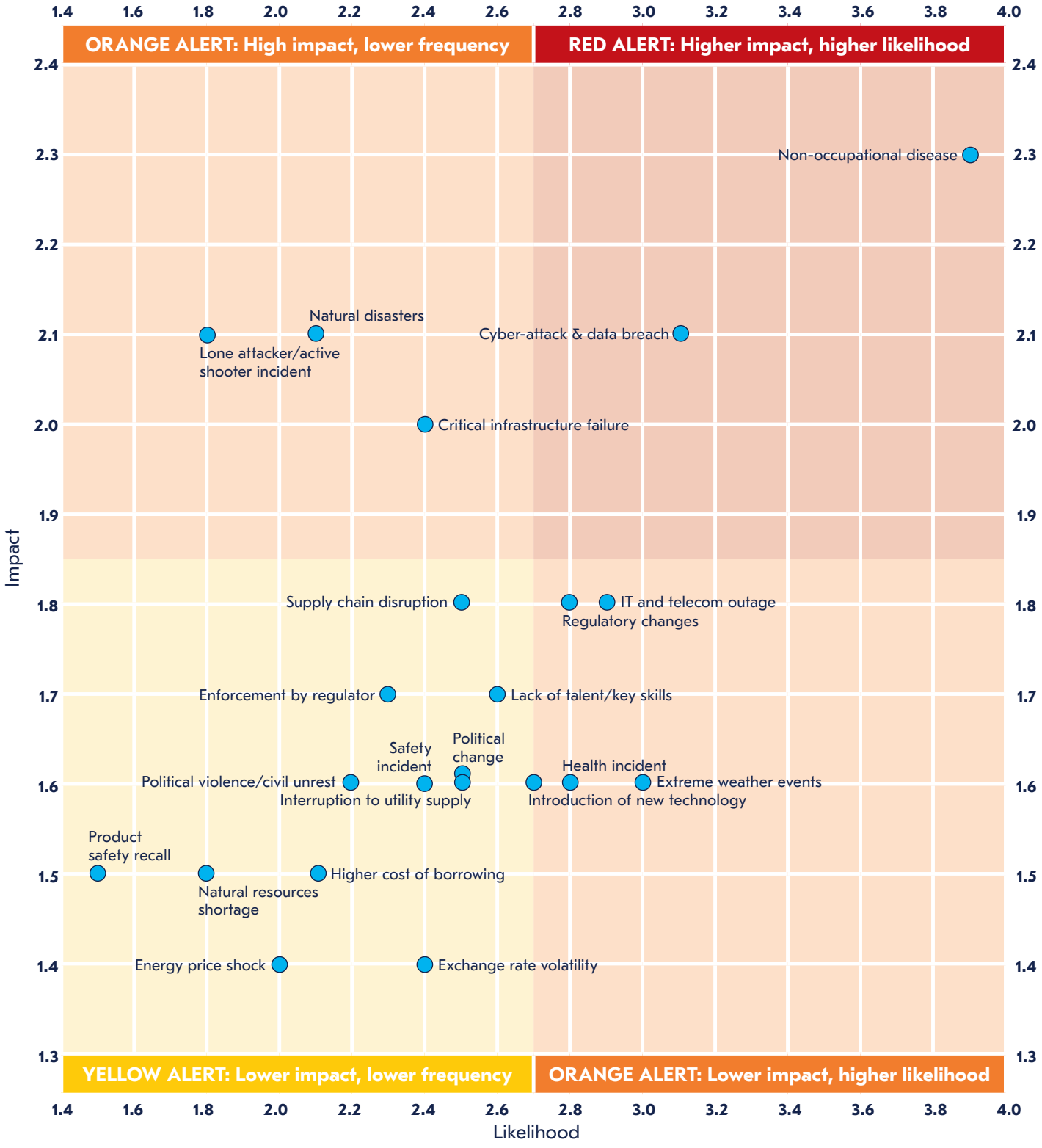


Figure 5. Risk and threat assessment: next twelve months

Consequences of disruptions

Consequences of disruptions

- The financial cost of disruption was only the third highest-rated consequence of disruption for 2020, with around half of organizations managing to finish 2020 without significant revenue losses.
- Loss of productivity was the greatest cause for disruption, although the quick adoption of new working practices (e.g. remote working) appear not to be the cause of this.
- Staff morale and wellbeing is set to be a major consideration for organizations during 2021 with employees impacted by feelings of isolation, losing colleagues to redundancy and balancing the challenges of disruption in domestic environments with their work.

Whilst news headlines focused on the financial consequences of COVID-19 to organizations during 2020, loss of revenue was only in third place this year when respondents were asked to consider impacts and consequences of disruptions experienced over the past year. Although the number experiencing revenue challenges was significantly higher than the previous year (2020: 51.7%; 2019: 36.3%), it does demonstrate that many organizations managed to get through 2020 with their balance sheets remaining in a strong position. However, organizations within certain sectors have been hit particularly badly: the leisure and hospitality sector, for example, has struggled with national rules ordering businesses to be closed. The retail sector too has been affected not just by reduced footfall in bricks and mortar stores, but also by changing purchasing patterns by consumers. Even the education sector, particularly the further education with a strong reliance on foreign students, has seen a devasting impact on financial performance in the past year.

"The major concern is actually being able to go forward through COVID. So the primary risk is just having enough funds to keep our quality standards up is hugely dependent on certain government funding, which is reducing all the time. We also need to pay for staff to carry additional things that they didn't carry before and get staff setup with the technology to provide their teaching online and research online; all those kind of things. We had a lot of students coming in from Europe. That's much reduced this year due to COVID. So, that has not just impacted us now, but it's also the concern of the long tail of this pandemic event going forward."

Risk Manager, Education, Ireland

This year's top disruption is once again loss of productivity, with 64.8% of organizations reporting it as an impact or consequence of disruption over the past year. Interestingly, however, the number reporting this dropped from the previous year (69.3%) which is an early demonstration that the new ways of working this year (e.g. remote working, minimal business travel) has led to staff being more productive in their roles.

Nevertheless, in an echo of the findings from the top causes of disruption, the second highest rated consequence of disruption this year is the negative impact on staff morale and wellbeing. Although this option was in second place last year, the increase of nearly 20 percentage points from 42.8% to 61.4% demonstrates the mental toll of 2020 on employees. Such findings are to be expected given the results of other studies recently carried out: a report by Westfield Health showed that the cost of absenteeism from work due for mental health reasons rose by £1.3bn to £14bn in the UK alone; a 10% percent rise year-on-year . Other economies reported similar findings. Whilst the findings are startling, the fact that organizations became better at supporting staff as the pandemic continued shows organizations are making tangible steps. The *BCI's Coronavirus Preparedness Report*, published fortnightly between March and May 2020 showed that by May, some 83% of organizations were considering staff mental health as part of their response, up from just two-thirds at the beginning of the crisis . With many organizations considering moving to fully remote or semi-remote working environments even as the pandemic risk starts to reduce, the concurrent issues on staff mental health will need to remain at the top of the agenda for organizations. Whilst many organizations have offered extra support services, training and literature about mental health, some larger organizations have gone a stage further. One interviewee highlighted how his organization had set up support funds for staff impacted by COVID-19. Encouragingly, many firms are keen for these measures to stay in place and will be using them to continually support staff going forward.

"One of the things the company setup was a resilience fund for COVID. This enabled staff, who have been financially impacted because of COVID, to receive funding. We've now expanded this initiative to other incidences that our staff were being affected by. Last year the resilience fund was made available during one of the larger typhoon events that hit the Philippines."

Head of Business Continuity Management, Real Estate, Asia

19. Smith, J (2021). Mental health related workplace absenteeism costs soared to £14bn in 2020. Workplace Insight [online]. Available at: https://workplaceinsight.net/mental-health-related-workplace-absenteeism-costs-soared-to-14bn-in-2020/ [accessed 24 February 2021]
20. BCI, The (2020). Coronavirus Preparedness Report — Issue 5. The BCI. Available at: https://www.thebci.org/resource/bci-coronavirus-organizational-preparedness-report---5th-edition-.html [accessed 24 February 2021].

The pandemic has prompted organizations to take an increased focus on their people

The COVID-19 pandemic has focussed organizations attention on their people in way we have not seen before. It is clear that those organizations that have been most successful in supporting their people, are also the ones that have been the most resilient overall. One of the biggest surprises for organizations is the fact that productivity was not unduly impacted by a move to home working. In fact, productivity impacts were actually less this year. Whilst this is a surprise for organizations, this is not a surprise for individual workers. There has been a lack of trust by organizations towards their workers, which has prevented a move to home or hybrid working models — a concern that workers will "take advantage" and not work as hard. This has proved not to be true. In fact, workers will step up and take extra responsibility if they are trusted. At an individual level, workers know this. What the COVID-19 pandemic has done is demonstrate this to organizations. This is an important realization and will be critical in the future job market. The best talent will only accept the roles where they are given flexibility to work in a way that suits them — where trust is evident.

Likewise, workers have seen first-hand how organizations look after their people and, in particular, support their mental health. The COVID-19 pandemic will have lasting impacts for the mental health of the current working population but also the younger generations who have yet to enter the job market. Organizations will need to not only continue to support their workers mental health but continually improve and enhance this provision. International standards, like the forthcoming ISO 45003 on psychological health and safety at work, will be important in achieving this. The provision of mentally and physically safe, healthy, and sustainable work, will be another critical differentiator in a highly competitive job market.

Another notable change in the list of consequences of disruptions between 2020 and 2021 is staff loss and/or displacement. 40.3% reported it as a consequence this year compared to just 20.9% in 2020. Many organizations have lost staff in the past year. In the United States, the unemployment rate hit a record high in April 2020 (14.7%) and, although it reduced dramatically to 6.7% by November, groups such as the Hispanic population and the younger generation remained disproportionately affected[21,22]. In the UK, the unemployment rate in the three months to November 2020 was at its highest level since 2016 - 5% - with the redundancy rate reaching a record high of 14.2 in the same three months[23]. Elsewhere in Europe, Spain reported jobless levels of 16.1%[24] whilst Greece, which had been enjoying a steady decline in the jobless rate from highs of 28% in 2013, saw unemployment rise again to 17.9% in June 2020[25]. For many organizations, redundancies were the only option to stave off liquidation as global lockdowns came into effect. This not only had the effect of directly losing talent, but the negative impact on remaining staff, if ill-managed, could lead to further talent attrition as the job market starts to open up again. A study carried out by Ceridian in November 2020 revealed that most of the American workforce - 64% - are either actively looking for a new position or would consider moving jobs if directly approached[26]. Such figures highlight the importance of ensuring remaining staff are provided with development opportunities and a supportive environment in which they can continue to flourish.

The loss of staff is not just a drain on the company's knowledge and the wellbeing of existing staff, but can have other knock on effects. An interviewee identified how they were now looking at the possibility of an insider threat as so many positions were going to be made redundant over the coming year.

"There's the insider threat as well. I know our organization's probably going to lose around 2,000 staff over the next 12 months; it's been flagged recently. So, again, depending on the nature of where people are and if they know the infrastructure and how to get into it, that's a big threat at the moment."

Senior Risk Analyst, Financial Services, Ireland

Sometimes, consequences of incidences — just like the incidences themselves — can be unexpected. The recent conflict between the Australian Government and Facebook resulted in some organizations being suddenly unable to impart vital information to their stakeholders.

"Recently Australians were blocked temporarily from reading or sharing news content on Facebook and our organisation's page was caught in that ban. We talk often about emerging risk and even though I had heard of the proposed changes to the law, we completely missed that one! Our Facebook site, which is one of the ways we use to communicate emergency warning messages and information to the public, was unable to be viewed. While it did come back up within a couple of hours, it was a good reminder that there's many types of disruptive events we can get caught up in."

Enterprise Risk Manager,
Emergency Services, Australia

Organizations are hopeful that the global situation will improve during 2021 as the health risks associated with COVID-19 start to reduce with the introduction of vaccines and new treatments. Caution is still being exercised by most, although we are seeing organizations start to invest again: the *BCI's Future of Business Continuity & Resilience report*[27] showed that 90% of Business Continuity professionals are hopeful of getting additional investment post-COVID, whilst the *BCI's 2021 Emergency Communications Report*[28] showed that of those organizations which did not have an emergency communications tool prior to COVID-19, 1 in 6 are now actively trialling a tool with a view to purchase.

21. Rushe, D & Sainato, M (2020). Year ends on low note as 787,000 more Americans file for unemployment. The Guardian [online]. Available at: https://www.theguardian.com/business/2020/dec/31/us-unemployment-december-coronavirus [accessed 24 February 2021].
22. Bureau of Labor Statistics (2021). The Employment Situation — January 2021. Department of Labor; US Government [online]. Available at: https://www.bls.gov/news.release/pdf/empsit.pdf [accessed 24 February 2021].
23. Denton, J (2021). U.K. unemployment hit its highest level since 2016, but London markets march higher. Marketwatch [online]. Available at: https://www.marketwatch.com/story/u-k-unemployment-hit-its-highest-level-since-2016-but-london-markets-march-higher-11611669844 [accessed 24 February 2021].
24. òmez, MV (2021). Spain shed 622,600 jobs and unemployment reached 16.13% in 2020. El Pais [online]. Available at: https://english.elpais.com/economy_and_business/2021-01-28/spain-shed-622600-jobs-and-unemployment-reached-1613-in-2020.html [accessed 24 February 2021].
25. National Statistical Service of Greece (2021). Greece Unemployment Rate. Traditing Economics [online]. Available at: https://tradingeconomics.com/greece/unemployment-rate [accessed 24 February 2021].
26. De Leon, R (2021). Majority of workers are looking for new jobs during Covid-19 pandemic. Here's why. CNBC [online]. Available at: https://www.cnbc.com/2020/11/13/majority-of-workers-looking-for-new-jobs-during-covid-19-heres-why.html [accessed 11 March 2021]
27. BCI, The (2020). The Future of Business Continuity & Resilience. The BCI. Available at: https://www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html [accessed 24 February 2021]
28. BCI, The (2021). Emergency Communications Report 2021. The BCI. Available at: https://www.thebci.org/resource/bci-emergency-communications-report-2021.html [accessed 24 February 2021].

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

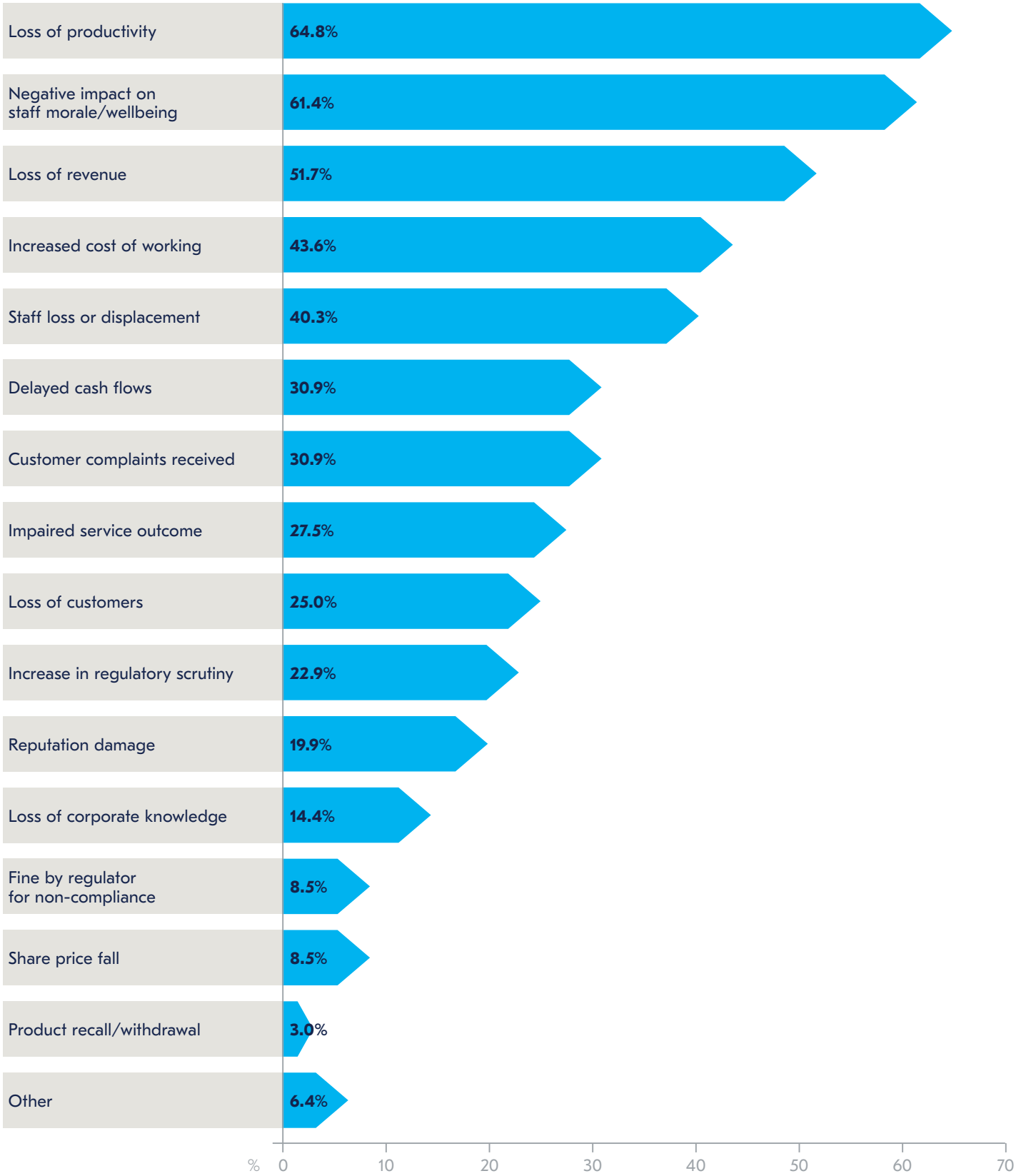


Figure 6. Which of the following impacts or consequences arose from the disruptions experienced in the last 12 months?

Benchmarking business continuity

Benchmarking business continuity

- COVID-19 has delayed many organizations' plans for ISO 22301, but more organizations are now using the standard as a framework.
- With certifications lapsing, organizations should consider opening dialogues with certification providers now to avoid the additional costs of restarting certification from scratch.
- Organizations have discussed how COVID-19 has helped to bring about better collaboration between departments, resulting in their organizations exhibiting a greater degree of resiliency. This is a reason for the BS 65000 Organizational Resilience standard being cited as one of the ten most used standards within organizations.
- Professionals have once again reported that aligning or certifying to ISO 22301 has brought about preferential insurance premiums and improved international trade.

Certifying or aligning to the ISO 22301 Business Continuity Management standard is used by organizations to ensure the quality of BC programmes, whilst also exhibiting the robustness of plans to external customers and stakeholders.

As a result, over half of respondents (52.7%) reported they use ISO 22301 as a framework but are not certified to it; a slight increase on 2020 (50.5%). Furthermore, of the 52.7% who use it as a framework, 9.8% are looking towards certification in 2021. Some interviewees discussed how they had been planning to certify in 2020 but had become consumed in their organization's response to COVID-19 and the decision had to be delayed. Others reported that their certification had lapsed during 2020 because of delayed or missed recertification audit appointments and they were planning to recertify as soon as possible. However, delaying beyond the six-month grace period is likely to lead to extra charges to reactivate the certification process.

The number of organizations delaying certification is a cause for concern: ComputerWeekly reported that across just three leading management system standards (ISO 9001, ISO 27001 and ISO 45001) there were an average of 2,500 certifications per month at risk of lapsing in the UK alone[29]. For organizations who are coming up to their recertification date, opening dialogues with certification bodies now can help explore options available. Some bodies have introduced methods of virtual certification, for example.

Moving towards remote delivery models to ensure continuity in global certification

BSI quickly pivoted to a remote delivery model to help ensure continuity to client certificates globally.

The organization quickly deployed a variety of technologies from desktop sharing and video conferencing tools (e.g. Zoom/Microsoft Teams) to more complex immersive technologies such as live streaming through mobile video technology connecting to a laptop or cellphone, as well as advanced live streams using smartglass technology.

Leveraging these approaches allows clients to maintain their current certification, reduce travel and gain increased access to global experts. This also allows us to transfer organizations' certifications from other accredited certification providers who may not be able to support these remote assessments.

I would encourage anyone who is uncertain about the upcoming audits and worried about their certificate expiry to engage with their certification body as soon as possible to discuss the options available.

Willy Fabritius
Global Head InfoSec, Privacy and Business Continuity
BSI

29. Scroxton, A (2020). Coronavirus: Thousands of ISO certifications set to lapse. ComputerWeekly [online]. Available at: https://www.computerweekly.com/news/252487843/Coronavirus-Thousands-of-ISO-certifications-set-to-lapse [accessed 24 February 2021].

Because many organizations are choosing to delay certification or are not renewing existing certifications, the number of organizations who report being certified to ISO 22301 fell back to 2018 levels (12.5%). However, with budgets reopening and professionals keen to reactivate delayed plans for certification, certification rates are likely to increase in 2021.

47.6%
We use ISO 22301 as a framework but are not certified to it.

5.1%
We use ISO 22301 as a framework, are not certified to it, but are in the process of getting certified.

12.5%
We use ISO 22301 as a framework and certify against it.

6.4%
We don't currently use ISO 22301 as a framework but we intend to move towards this during 2021

28.3%
We don't use ISO 22301 as a framework and have no plans to move towards this during 2021

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

Organizations aligning or certifying to ISO 22301 exhibit a higher degree of resiliency

Those organizations who do certify or align themselves to ISO 22301 exhibit higher levels of resiliency. When considering a "staple" disruption such as an extreme weather event, just 3.8% of those who were certified or aligned to ISO 22301 reported a "major" or "extreme" impact on their organizations compared to 7.1% who were not. 8.3% of organizations who were not certified or aligned reported "extreme" disruption to supply chains in 2020 compared to 3.8% of organizations who were certified/aligned.

Some organizations reported that there was less of a need to certify to the ISO 22301 as they already had to adhere to industry or country regulations related to business continuity and resilience. 10.5% of respondents from the highly regulated financial services sector report being certified to ISO 22301 compared to the 30.6% of those from the IT sector. A good example of this is in Australasia where alignment levels were the highest in the world at 88.0%, yet interview respondents in the region reported there was "no certification requirement" to the international standard as they had to certify to country-specific standards instead.

"My personal feeling is, and I stated this when I made the case for using ISO 22301, is that we should be using it as a benchmark for our critical third-party providers. What you'll typically see with suppliers is alignment to ISO 27001 which is fine for IT RTO/RPO. But we need our critical third parties to understand what would happen if they lost the building, they lost a critical supplier, they lost a critical utility supplier. And that's not captured."

Senior Risk Analyst,
Financial Services, Ireland

Information security and risk management standards remain the most popular standards

The top four standards organizations report certifying or aligning towards are ISO 27001 (Information Security Management), ISO 31000 (Risk Management), ISO 9001 (Quality Management Systems) and ISO 14001 (Environmental Management). Many organizations cited that one of the reasons for not certifying to ISO 22301 was because they required certification to other standards due to stakeholder demands and/or expectation. The most widely used regional standard is the NFPA/CSA Z1600 Disaster/Emergency Management standard in the United States and Canada. However, a notable new entry to the list this year is the BS 65000 Organizational Resilience standard. The British standard has seen a renewed level of interest this year in the wake of COVID-19, with interviewees reporting how their organizations were increasingly looking to move towards the concept of overall organizational resilience and were seeking a framework to start developing the concept within their own organizations.

"We have compliance obligations and guidelines in Western Australia that require us to have effective risk management and business continuity arrangements in place, but there is no legislative requirement. We take an integrated approach to risk management to ensure all areas of the business effectively recognise and manage risk, and we adopt good practices from a number of relevant standards including those related to safety, security and resilience, and risk."

Enterprise Risk Manager, Emergency Services, Australia

"As a New Zealand entity with an Australian parent we comply with the [Australian Prudential Regulation Authority] standard CPS 232. The standard is Australia's version of the Good Practice Guide and it's that standard that drives the requirement for a business continuity program."

Business Continuity Manager, Financial Services, New Zealand

Do you use any other management system standards to manage risk and/or reslience?

Other management standards used: Top 10		
1	ISO 27001	Information Security
2	ISO 31000	Risk Management
3	ISO 9001	Quality Management Systems
4	ISO 14001	Environmental Management
5	NFPA/CSA Z1600	Disaster/Emergency Management
6	ISO 45001	Occupational Health & Safety
7	ISO 14971	Risk Management for Medical Devices
8	ISO 13485	Quality Management Systems for Medical Devices
9	ISO 20000	IT Service Management
10	BS 65000	Organizational Resilience

Figure 8. Do you use any other management system standards to manage risk and/or reslience?

Certification can help to bring tangible benefits to balance sheets

For those organizations who have certified towards ISO 22301, the top two reasons given are that it increases an organization's resilience (71.8%) and that it enables consistent BCM measurement and monitoring (69.0%). Both these options took the same top two positions in the 2020 Horizon Scan report demonstrating that the primary motives for certifying have remained unchanged during the pandemic period. The third most selected option this year, however, is to ensure alignment with industry peers (56.3%) further demonstrating the importance of being able to demonstrate certification within certain industries such as the IT sector where a third of organizations are certified. Over a half (52.3%) said that certification helps stakeholders to better manage risks, indicating that proof of certification is sometimes requested by stakeholders.

This year, the number of organizations who report certification has led to helping to reduce insurance costs has risen to 40.9% (2019: 27.5%) whilst those indicating that it had helped to improve international trade rose to 36.6% (2019: 25.2%). With 49.3% claiming it improves customer satisfaction and 52.1% saying it enables faster recovery from disruption, the benefits of certification to an organization's balance sheet are therefore quantifiable. For those organizations who are finding it difficult to get management buy-in to certifying to ISO 22301, using statistics such as these could help make the argument easier.

What benefits does certification provide to you and your organization?

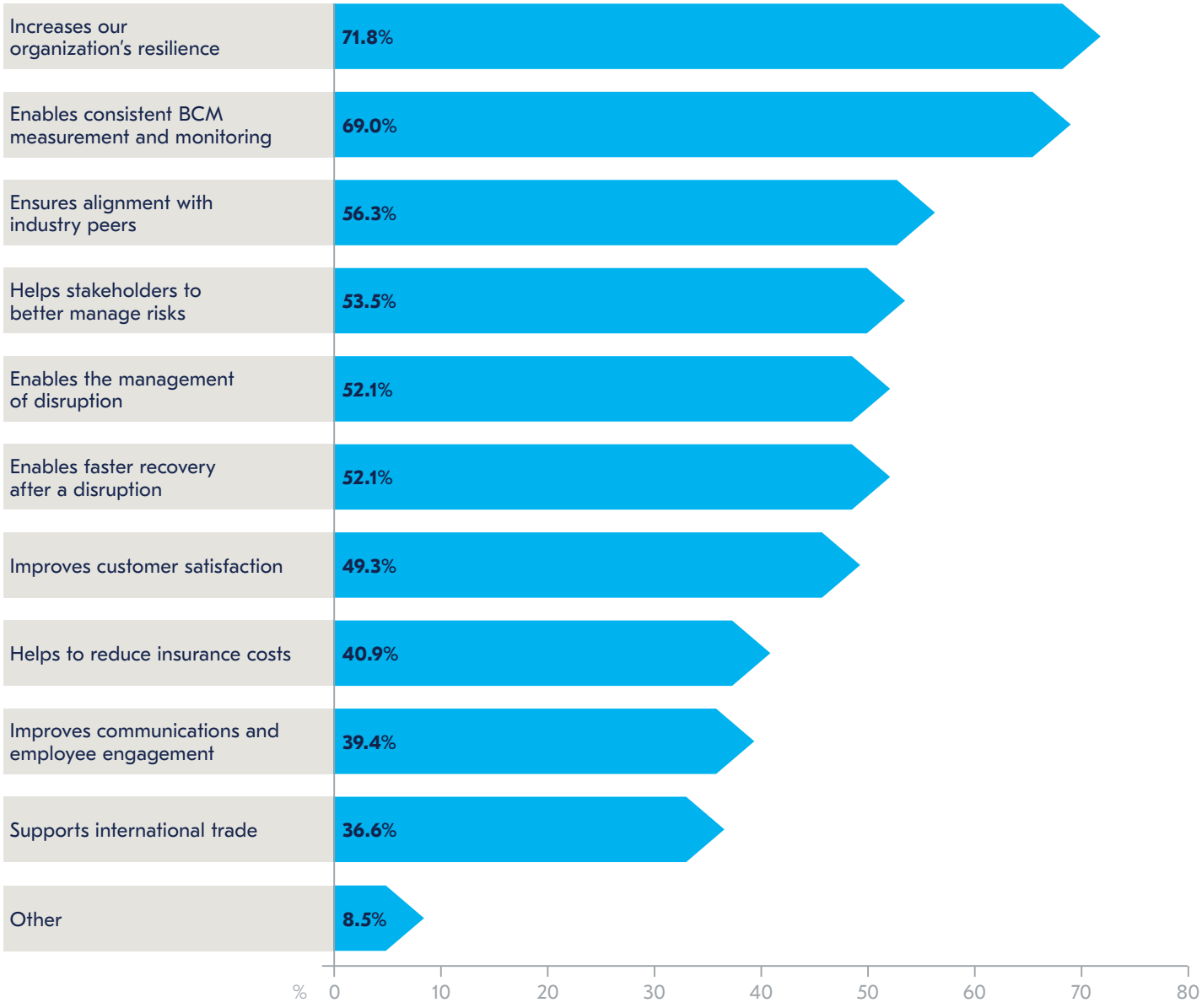


Figure 9. What benefits does certification provide to you and your organization?

Lack of business requirement tops list of reasons for non-certification

For those organizations who do not certify to ISO 22301, the primary reason cited by nearly two-thirds of respondents was the lack of business requirement (60.0%). Many organizations reported that whilst they were often asked for proof of alignment to ISO 22301 at contract stage with a new customer, the requirement to certify was not something they ever had requested from them. Others reported established and successful BC programmes were already in place, often using the ISO 22301 as a framework, and certification was not something required. This was particularly the case where management were already satisfied with the processes in place.

A third of organizations (33.9%) said they had not certified due to a lack of external drivers. Indeed, for those in industries where certification levels were low, where organizations were based in countries where local standards prevailed or the organization had no customer requirement, or the investment of certification was not a viable expense for the organization.

"For us I think it's a better decision to be aligned; and we are quite closely aligned to ISO 22301. However, the certification in itself doesn't give us anything at this time. It's not like we're competing with other markets for other customers where certification may be a differentiator against our competitors. We're not developing products or trying to sell stuff. For independence, we also have external auditors to, on occasion, review our BCMS. That's enough for us."

Business Continuity Manager, Public Sector, United Kingdom

"A couple of our critical third parties are certified but the bank, other than it holds a bigger bank's money or pushes money, doesn't have a requirement to be certified. It should be aligned, and they should look for evidence that it's aligned, but they don't. Again, I think that it's a culture within the Irish market. It's all about how can we do business continuity with as little or as minimal effort as possible. So, being aligned or certified in a lot of places just isn't on the cards."

Senior Risk Analyst, Financial Services, Ireland

"Our organisation stood up an advisory committee initially in the early stages, as Covid started to gain traction across Risk activities. It created a pan-group entity, that was borne from a similar approach taken to a possible 'No Deal' Brexit about 12 months earlier. Once Covid became a nightly news item, suddenly we jumped into a 'Silver' response. Although there was a Pandemic Plan in place, as with the infamous saying, 'no plan survives the meeting with reality' as it was deemed 'not fit for purpose' – as I'm sure those that had a Pandemic Plan will have found, especially if not reviewed since SARS or Ebola alerts from a few years back. So it got tossed and they reverted to a 'Severe Weather' Plan. This was because the impacts to staff (denial of access etc.) had been well road tested due to recent weather events. People knew their roles and responsibilities from such weather events, so the biggest hurdle was the change of thinking to pandemic planning / response. One critical element was timelines – there was just no way to know how long this pandemic would last – so it was difficult as the external environment was changing all the time with different outlooks or information. If you use the Spanish Flu as a predictor, it was about 22 months approximately. That's a huge change in planning a response, whereby you might have previously looked at disruptions in days, weeks and at a push, months. As the business evolved, so did technology. They started to look at what would happen if we had to work from home from a protracted period."

Senior Risk Analyst, Financial Services, Ireland

A quarter of organizations (25.2%) reported there was no management commitment to certifying to the standard, particularly if the organization was already aligning to other management standards in the areas of IT disaster recovery and risk, for example.

Cost, however, does remain a barrier to nearly a third (29.1%) of organizations who report they have no budget available to certify. For those organizations, approaching management with the tangible benefits of certification as highlighted in figure 9 could be one method of gaining management buy in. Other methods could be exploring whether certification will result in preferential rates and/or terms from suppliers or speaking to insurers to determine whether a reduction in premium would be considered if certification could be obtained. With the deep impacts felt in organizations' supply chains over the past year, exploring options such as certification could be considered an advisable approach.

"Last year we had an internal and external consultant come in and do a gap analysis. I said that the ISO standard was something we'd be interested in and we were told we should go for the ISO standard and I'd stand a very, very high likelihood of getting it. But upon doing a bit more investigation and market analysis of how much it cost, how frequently you needed to do it, it became a nice to have, but the view of our leadership was that particularly in a post pandemic year it just wasn't viable because of heightened sensitivity around what we're spending money on. We couldn't justify the return on investment at this time, particularly in our sector at this time."

Business Continuity Manager, Automotive, Canada

What are your reasons for not being certified or having no plans to be certified to ISO 22301?

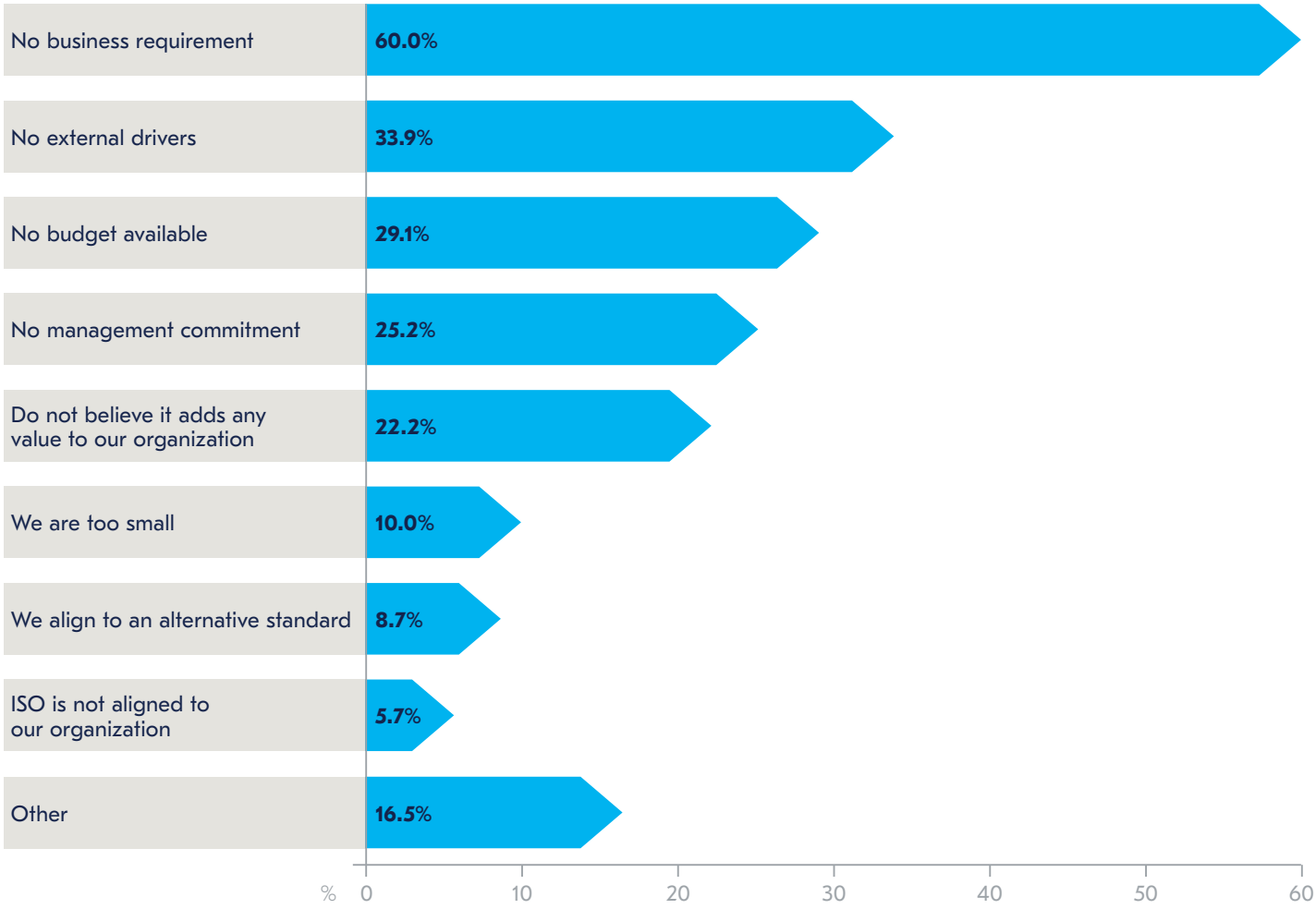


Figure 10. What are your reasons for not being certified or having no plans to be certified to ISO 22301?

Benchmarking longer term trend analysis

Benchmarking longer term trend analysis

- The number of organizations performing longer-term trend analysis has risen to an all-time high (81.3%) with more than half now carrying out analysis via a centralized unit.
- The use of different tools for risk analysis has increased across the board. COVID-19 has encouraged organizations to be more thorough with their trend analyses and explore new sources of information.
- Professionals are more confident that they will get increased investment in their BC programmes this year than they were this time last year. Many professionals report management's positive experience with BC departments during the pandemic has led to more funding becoming available.

COVID-19 has been a positive force for change within organizations, with management teams pushing for longer-term trend analysis. Last year's report saw a disappointing fall in the number of organizations who conduct longer term trend analysis to 76.9%, whilst this year the figure has reached an all-time high of 81.3%. The biggest increase was seen in those organizations performing centralized analysis, where 52.8% reported their analysis was carried out by a centralized function (2019: 45.9%). The increased attention on conducting analysis was further discussed in interviews, where professionals told how their COVID-19 had been the precipitator to introducing a more centralized analysis programme, drawing on all parts of the business. Others reported how management had become more demanding of seeing the outputs of trend analysis due to heightened levels of uncertainty. However, there were still some organizations who still struggle to get management buy-in to allow centralization of processes to take place.

" have been with the company for almost 15 years and for 14 of those years, I've been pretty vocal about the need to centralize this function. A centralized business continuity organization would really serve many purposes, not least of which is getting everyone to the same level of expertise and maturity with the capability to meet the same events head on. Clearly that's not where we are today. Also, the farther we get past the real heavy weight of the pandemic, I can see management already sliding back into that siloed, isolating their own stuff approach."

Business Continuity Manager,
Technology, United States

Despite the positive trend noted in 2020, 1 in 6 respondents (16.7%) reported their organization did not carry out longer term trend analysis at all. Although some interviewees told how risk monitoring was still done in an "ad hoc" way or that national risk registers were downloaded as a routine process, but the lack of a managed process in place will leave organizations exposed to the wider risk landscape.

For some organizations, good horizon scanning enabled them to consider the impact a pandemic would have on their organization before news of COVID-19 was available. An astute Business Continuity professional interviewed for the project noted that a pandemic was the most likely of perceived hazards to occur in the next five years in the 2017 National Risk Register in November 2019 and flagged this as an issue to their organization.

"I wrote to my risk management colleagues on 12 November 2019 after we had just had our first emerging risk workshop. It was run by risk management and included business heads from the UK and from the US. At the time, cyber was up there, as it has been for many years now, together with climate change and other potential threats. My note flagged that pandemic was the most likely of perceived hazards on the National Risk Register 2017 to be realised within the next five years — so by 2022. I believed we needed to get a greater weighting, not just for our own staff but all our stakeholders as well. It feels like I had a crystal ball. By the time the pandemic was on the radar, we'd already started to requisition additional laptops and to prepare staff to work remotely. So when we had to switch to remote working, it was a relatively seamless operation."

Group Business Continuity Manager,
Financial Services, United Kingdom

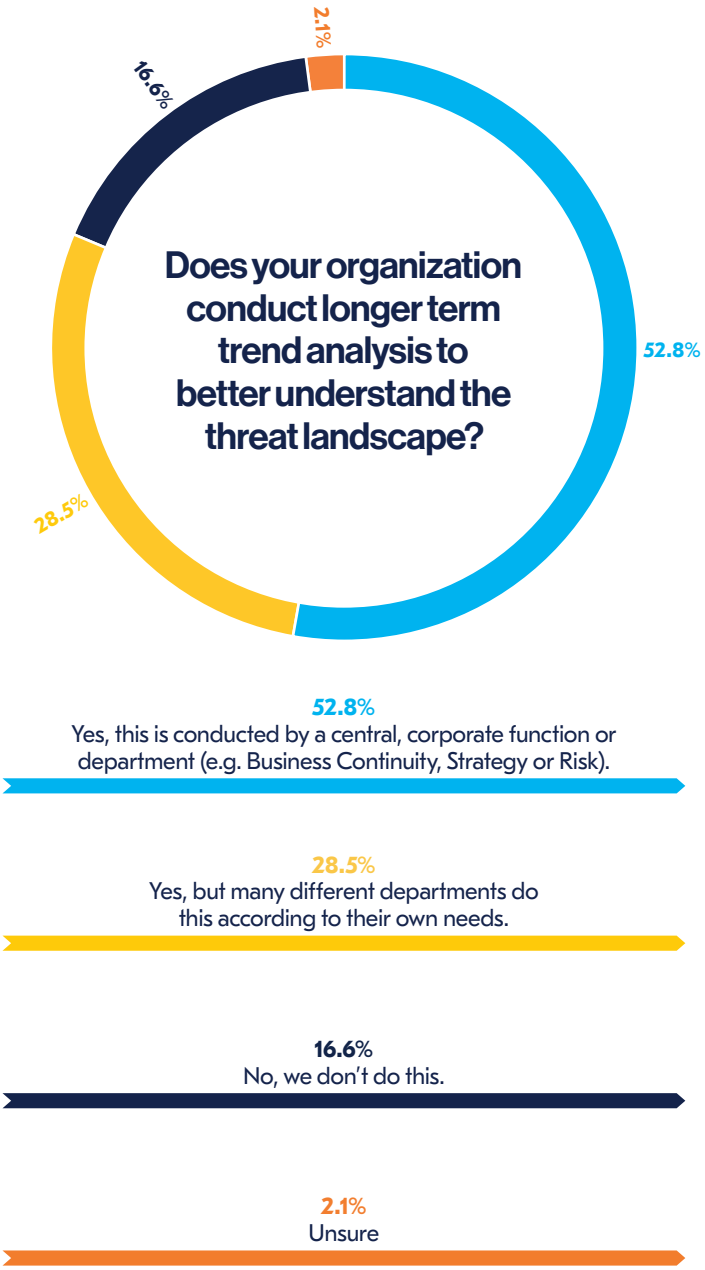


Figure 11. Does your organization conduct longer term trend analysis to better understand the threat landscape?

Although more organizations are now carrying out longer term trend analysis, nearly a quarter of respondents (24.0%) said they did not have access to the outputs of longer-term trend analysis to input into their programme. For a BC programme to be able to protect the organization against existing and emerging threats, access to this trend analysis is vital. Many professionals reported how silos between departments had been broken down and better communication lines had been created because of COVID-19. Employing these same techniques with other teams during the pandemic could help to achieve better access to the information used for longer term trend analysis, even if in a shortened format. In larger organizations, ownership of the risk register is normally by the Chief Risk Officer whereas in smaller organizations, it tends to be with the financial director or accountant[30].

However, even for those who do have sight of the risk register, there are frequently issues with that as well.

> **"The risk registers are not used as a rigorous management tool. They're used as "risk admiration" i.e. credit for having a nice looking risk register "Oh, that's a lovely risk register. That's nice." Rather than saying, what are the mitigation tasks? How do we track actions and where is evidence that mitigations are effective?"**
>
> Business Continuity Manager, Public Sector, United Kingdom

30. Morton, T (2010). The Basic Principles of Compiling a Risk Register for Smaller Companies. ACCA [online]. Available at: http://web.actuaries.ie/sites/default/files/erm-resources/tech_afb_trr.pdf [accessed 24 February 2021].

For those that do not have access to their organizations' own analysis, resilience professionals would be advised to still make use of the array of free resources available such as reports like the BCI Horizon Scan, national risk registers and the OECD cross-country perspectives of global risk[31].

Strong peer-to-peer relationships can also be useful in assessing the risk landscape: communication with other resilience professionals in BCI Chapter Meetings or online industry events, for example, can help to provide a more rounded view of the risk landscape. Other views can also be gathered by opening up communication channels with customers, suppliers and local business forums.

41.9%
Yes, I'm aware of the outputs and use them

32.3%
Yes, I help develop the analysis in the first place

24.0%
No, I do not have access to this information

1.8%
No, I don't see the value of this information

Figure 12. As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme?

31. OECD (2021). OECD Risk Website. https://www.oecd.org/gov/risk/ [accessed 24 February 2021].

Practitioners are exploring new information sources to get a broader view of the risk landscape

Practitioners use a variety of tools for trend analysis, and the percentages have increased for each information source this year. This is indicative of the general trend of organizations performing a greater degree of risk analysis in 2020 than has ever been recorded in this report. 91.7% of professionals use an internal risk and threat assessment (2019: 86.0%) and 71.7% use risk registers (2019: 62.5%). One of the sharpest increases has been the use of external reports and industry insights: just 58.2% used these as a source in 2019, but this has increased to 71.7% this year. This is perhaps a reflection on a high proportion of professionals working remotely and consuming knowledge through printed/electronic formats which would normally have been obtained through face-to-face meetings and/or industry conferences. Nevertheless, the availability of virtual industry conferences this year means 58.7% of respondents still use these as an information source (2019: 50.1%). The only source which has seen a slight decline in use this year is the use of risk assessment software: 16.1% of professionals reported using it compared to 17.0% in 2019. However, with the augmented interest in 2020 in better understanding the risk landscape, a natural progression for many organizations could be to invest in specialist technology solutions as budgets start to free up again.

An interviewee discussed how they developed their own threat assessment process to identify upcoming threats or advanced threats within the primary locations. Another mentioned how they use industry analysts to help develop their threat landscape.

> **"I'm trying to develop a threat assessment process to identify upcoming threats or advanced threats within our primary locations. We have around 20 primary locations around the globe and I'm looking at what the headlines are in those areas. What is the weather going to be like for the next seven days? What do I need to be on the lookout for? Where do I need to focus my daily threat assessment efforts? I think this will help with our short-term risk planning and provide early warning of getting hit by something I'm not expecting."**
>
> Business Continuity Manager, Technology, United States

"We've had long standing full access to Gartner and all their analysis and reports. So this year we've been having more conversations with Gartner analysts concerning things both within the industry, and specific in what we're doing. We also went to a risk management software provider in 2019. That's new. That's covering our central risk group and the BC area, and now they're adding the risk module into ServiceNow we can do even more. We're also increasing our vendor security assessments and risk assessments of all of our vendors whilst this is going on. How stable are the vendors that we're using? We're consolidating down on the number of vendors, so I would say that's being more formalized from the process stage."

Director of IT & Resiliency, Financial Services, United States

"We've accessed different COVID-related tools. We found out about a product that is being evolved internally from a medical risk perspective. We saw this demonstrated to us a few weeks ago and both my colleague and I were really excited by this because the potential for it is very helpful not just from a medical perspective in terms of disease but from a risk based one. We've regularly used resources like John Hopkins and others and gone into various other websites that we've found to collate COVID related information. Generally, we've expanded what we've looked at in terms of what's come to market in various theatres of risk."

Head of Risk, Healthcare, United States

Some professionals discussed how they used their advisory network (e.g. solicitors, insurers or accountants) to help with their risk analysis or using reports from sectors where risk scanning is more mature to help gain insights, whilst others had a specialist team within their organizations who were tasked to do external horizon scanning and risk monitoring.

"There are a lot of reports available in the market. Our insurance providers also help us in terms of giving us information about the latest trending risks; what is happening in the world. We also use publicly available information like World Economic Forum, risk reports and things like that. Also, from a risk perspective, the banking industry are much more mature so I do look to them in terms of seeing what other things are happening, whether it's artificial intelligence, blockchain and things like that. These things may not impact today, but may go up in the future and we have to be prepared."

Head of Business Continuity, Electronics, United Kingdom

"We have a small internal enterprise risk management team and every day they're doing external horizon scanning. They own enterprise risk management, predicting risks, and putting themes and trends together. The BCM program works closely with them, meeting quarterly and as the global risk environment changes. We own the Business Continuity Management Risk and we have a great collaboration; they'll consult with us on emerging risks, we'll consult with them on geopolitical risks."

Business Continuity Manager, Consumer Goods, United States

The use of social media has also increased this year for risk monitoring purposes, particularly monitoring for near term risks or incidents occurring on the ground. Although information gathered from social media should be used with care, it can provide an early alert of an unfolding situation where company operations may be affected.

"We actually find social media monitoring very useful, and I can give a good example. There was a stabbing in Sydney a few years ago, which was outside one of our offices. The office management were not aware this was occurring as they occupied a top-level floor in the building. We were able to flag this to them and have the building locked down. Based on reporting from social media, we were able to send out welfare checks to staff regarding this evolving incident."

Head of Business Continuity Management, Real Estate, Asia

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

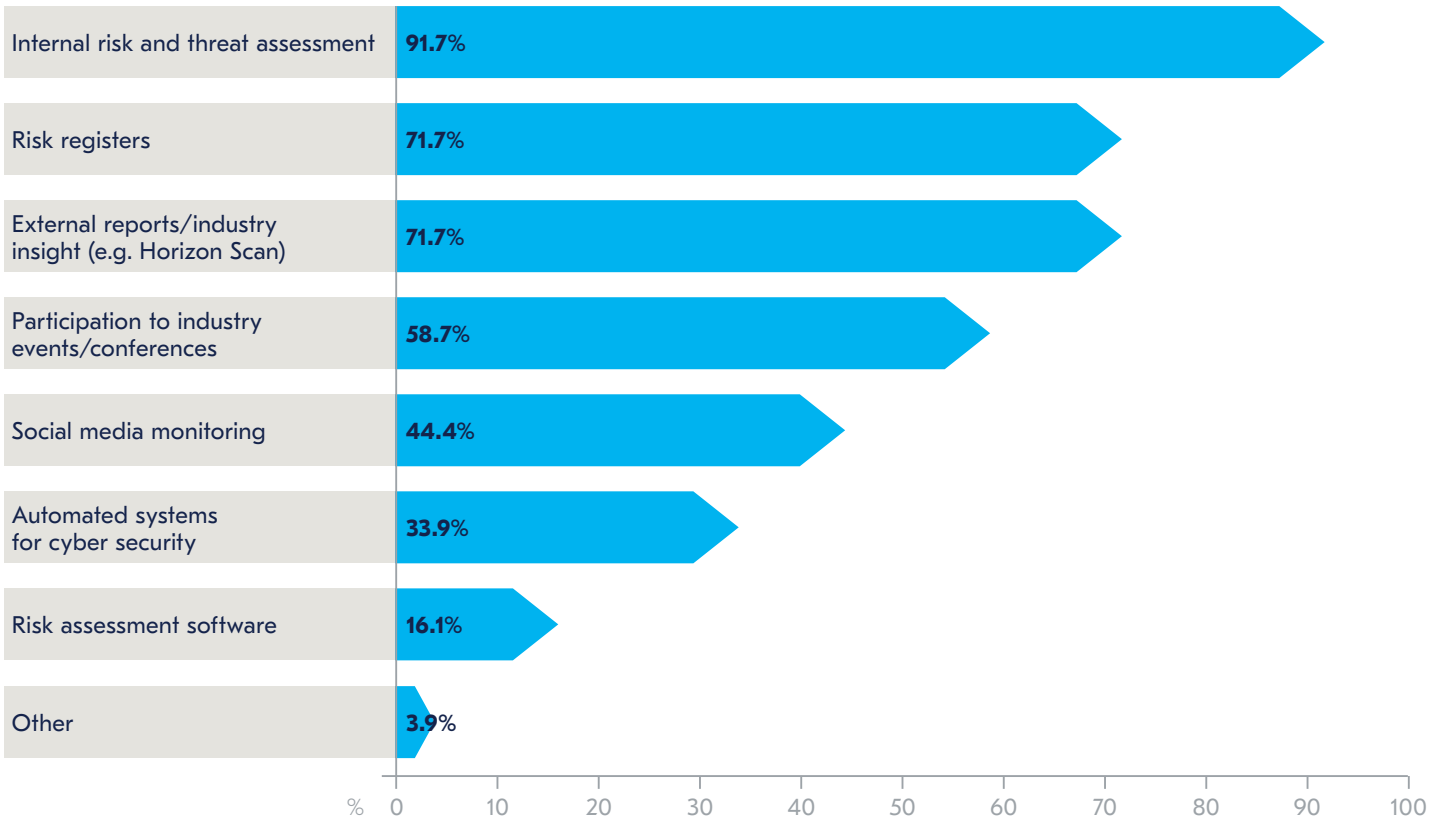


Figure 13. How do you conduct a trend analysis of the risks and threats to your organization?

More than half of respondents (53.3%) reported their organization's Business Continuity Management programme was now a mature programme, being in place for more than five years (2019: 49.1%). In contrast, 28.1% reported their programme had been in place for less than three years, down from 33.9% in 2019. The increasing levels of maturity in organizations' BC programmes is likely to be one of the reasons why levels of risk monitoring have increased in organizations as well as the increasing number of organizations who are using the ISO 22301 standard as a framework.

An interviewee reported how he has only been in the role for 18 months and was still building the programme to a mature level, which was not without challenge. However, thanks to the Government being proactive regarding business continuity, it was helping him to build a strong programme within his organization.

11.7%
1 year — this is still new for the business

16.9%
2-3 years — this has been recently established

18.2%
3-5 years — this is a well-established programme

53.3%
5+ years — this is a mature programme

Figure 14. How long have you been engaging in business continuity management planning for?

After an unprecedented year, it is important to reflect and learn to support future analysis.

In 2020, BSI's Supply Chain Intelligence explored the risks associated with protests that occurred in each region of the world. While different events initially triggered these protests (e.g. anti-lockdown measures in Israel or changes to farm laws in India), a common trend underlying this embedded social discontent is widening inequality and poor living standards.

More recently, frustrated demonstrators across the world have taken to the streets to protest the reimplementation of national lockdown measures by countries in response to emerging variants of the COVID-19 virus.

These protests have proven to be problematic for political structures, as single-issue anti-lockdown protests or industry-specific labour strikes have evolved into multi-issue anti-government protests that impact broader, long-term disruption to business operations.

The aftermath of the COVID-19 pandemic and the negative economic impact on national economies is likely to increase inequality within populations and trigger further unrest in the year to come.

It is important to consider these risks in long-trend analysis and that organizations manage appropriate, and current, plans that are flexible enough to apply to multiple potential situations that are focused to provide concrete steps and actions that employees can take to mitigate risk.

BSI Supply Chain Intelligence

Investment in business continuity and resilience looks set to increase in 2021

Despite the challenges of 2020, the increased level of visibility that resilience professionals have gained during the pandemic period has led to 30.9% of respondents indicating that investment will increase in their BC programmes in 2021. This is a slight increase on last year's figure of 29.2%. Just 9.1% of respondents believe that budgets will be cut in 2021, a similar figure to 2019 (9.0%). Some interviewees did report that funding was going to be available for other resilience functions over the coming year, but there was no budget specifically set aside for business continuity.

"Despite very significant impacts to operating budgets, our organization has seen the value in investing in the BCM Team, specifically training. It is a reasonably new team, with most new members not having any formal BCM training. With the funding for training, it gives team members access to CBCI and DBCI qualifications. The CBCI is a great introduction qualification as it allows the team members to get a solid foundation of knowledge under their belts. Add this to the day-to-day experience, and the team strength and knowledge is being built on. The DBCI gives individuals who see BCM as a career pathway an opportunity to go beyond the CBCI and become solid specialists in BCM. By becoming subject matter specialists, the organization can have confidence that it has a well-trained and knowledgeable cohort when it comes to developing and maturing its BCM programme."

Senior Risk Analyst, Financial Services, Ireland

Indeed, interviewees discussed how budgets were already being increased for the coming year, with some reporting that they already had new positions approved within their teams. Equally, however, many teams remain under pressure to deliver with reduced budgets, particularly in sectors which have been impacted hard by COVID-19: two-thirds of charities/not-for-profit organizations (66.7%) believe investment in BC programmes will be cut this year. Conversely, for those industries where growth prospects are high, investment looks set to increase: 60.0% of transport and logistics organizations believe budgets will be increased over the next year, with 41.7% of professionals within the IT sector hopeful of budget increases over the coming year.

"That investment will specifically be in resilience. The investment we are making is in supply chain modelling to understand where vulnerabilities exist and how we can build resilience. So, I would say we're moving towards building resilience in an effective and efficient way. But there are so many other benefits, not just only to business continuity management but to the business results because we will build that resilience together with flexibility and agility. So that's where the investment is happening."

Business Continuity Manager, Consumer Goods, United States

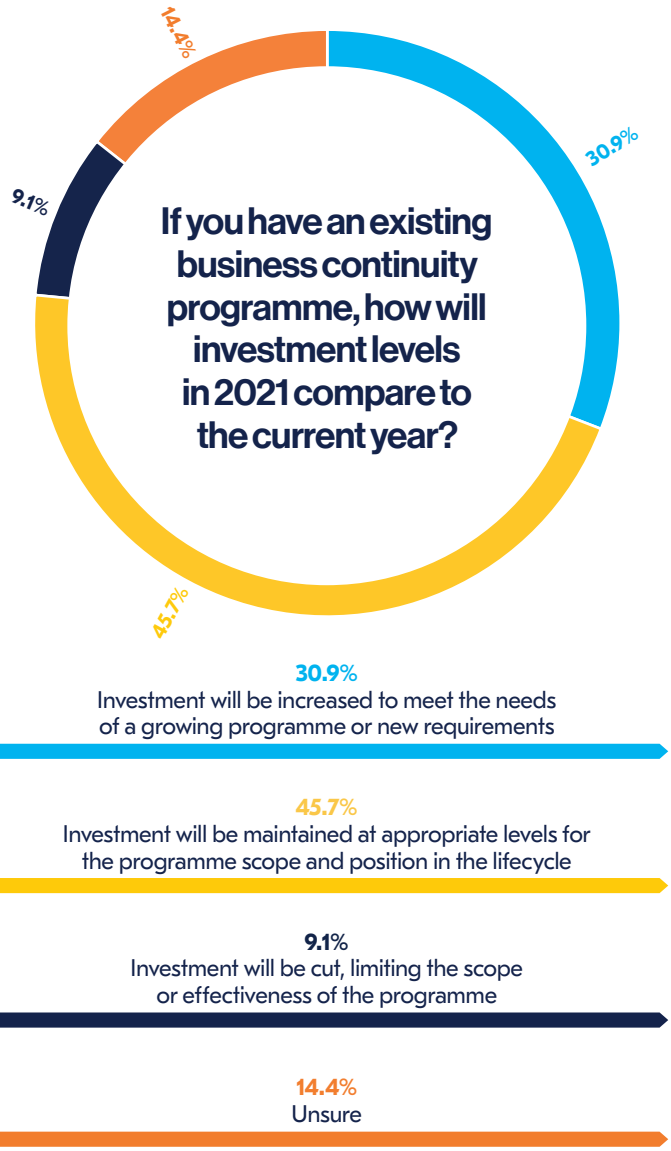
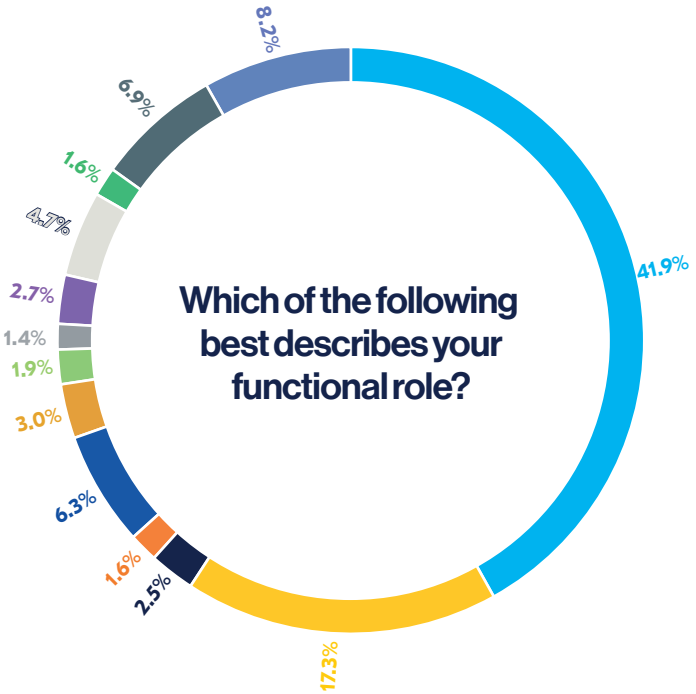


Figure 15. If you have an existing business continuity programme, how will investment levels in 2021 compare to the current year?

Annex



41.9% Business Continuity

17.3% Risk Management

2.5% Internal Audit

1.6% Line of Business/ Service Directorate

6.3% Quality/Business Improvement

3.0% Health & Safety management

1.9% Emergency Planning

1.4% Security (physical)

2.7% Cyber/Information security

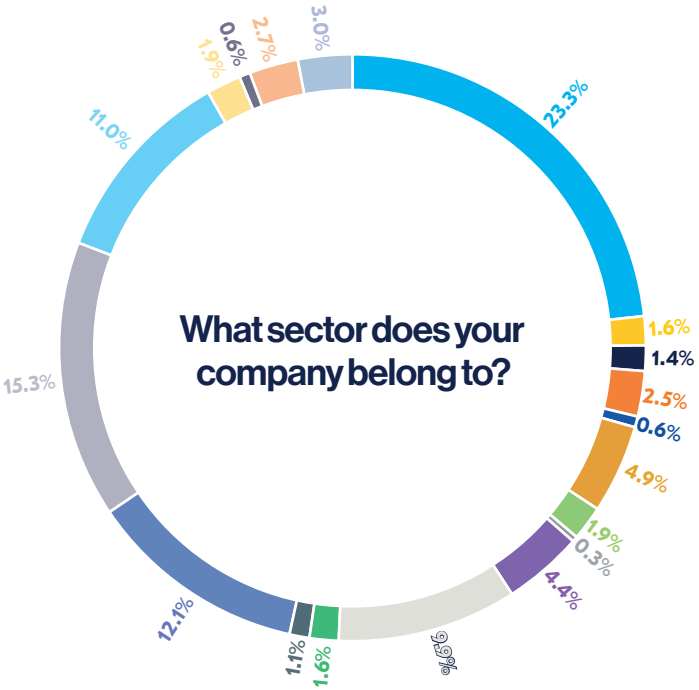
4.7% IT Disaster Recovery/ IT Service Continuity

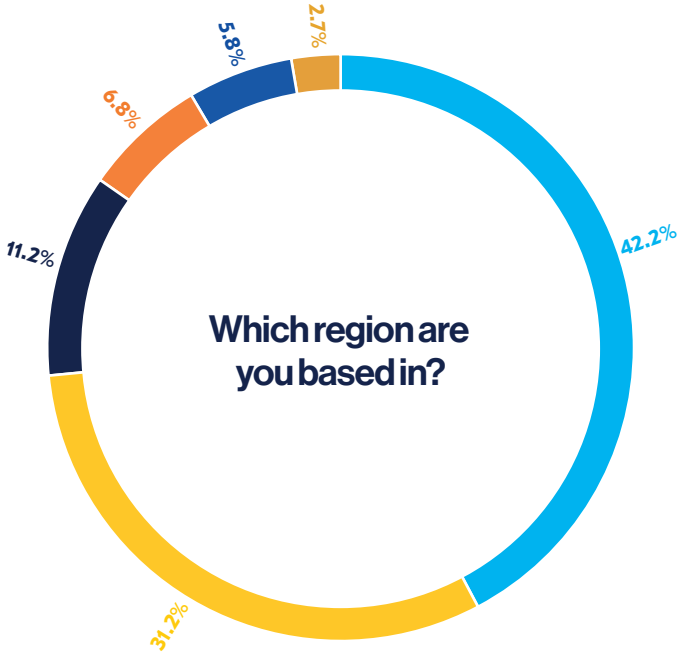
1.6% Crisis Management

6.9% Top Management

8.2% Other

Figure 16. Which of the following best describes your functional role?





23.3% Banking and finance

1.4% Creative industries

0.6% Emergency services

1.9% Engineering and infrastructure

4.4% Healthcare

1.6% Law enforcement and security

12.1% Manufacturing

11.0% Public services, government and administration

0.6% Retail and wholesale

3.0% Transport and logistics

1.6% Charity/Not for profit

2.5% Education and training

4.9% Energy and utilities

0.3% Environment and agriculture

9.9% Information technology

1.1% Leisure and hospitality

15.3% Professional services

1.9% Real estate and construction

2.7% Science and pharmaceuticals

42.2% Europe

31.2% Americas

11.2% Asia

6.8% Australasia

5.8% Africa

2.7% Middle East

Figure 17. What sector does your company belong to?

Figure 18. Which region are you based in?

9.3% 1-10

3.6% 11-20

4.4% 21-50

3.6% 51-100

6.0% 101-250

6.3% 251-500

5.8% 501 - 1,000

19.5% 1,001 - 5,000

13.2% 5,001 - 10,000

13.2% 10,001 - 50,000

6.9% 50,001 - 100,000

8.5% More than 100,000

11.0% Less than €1 million

10.7% €1-10 million

3.3% €11-25 million

3.3% €26-50 million

3.0% €51-100 million

3.0% €101-250 million

4.4% €251-500 million

6.9% €501 million-€1 billion

13.4% €1-10 billion

6.0% €11-50 billion

4.7% Greater than €50 billion

30.4% I don't know

Figure 19. Approximately how many employees are there in your organization globally?

Figure 20. What is the approximate global annual turnover of your organization?

Asia Pacific: past twelve months

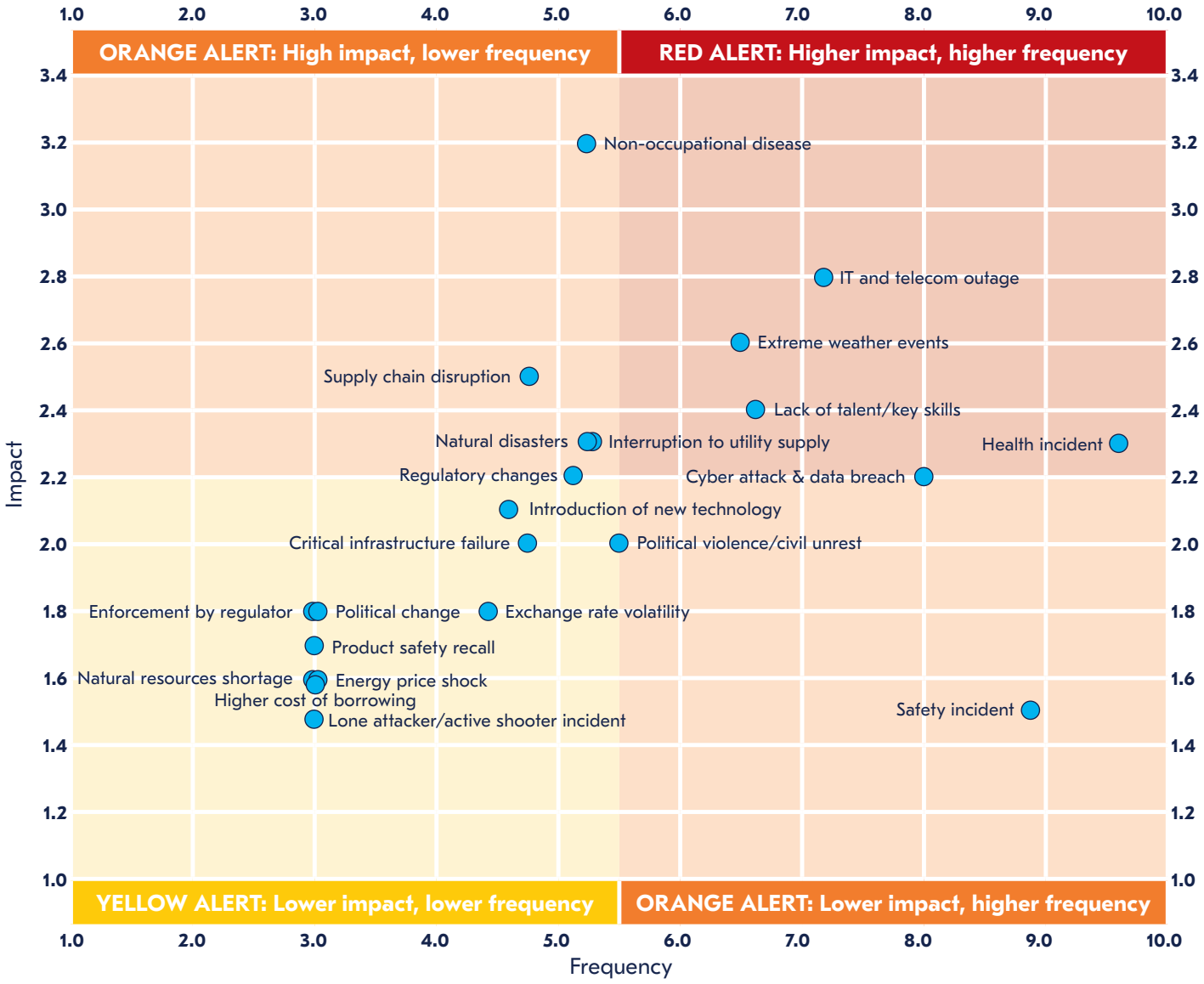


Figure 21. Risk and threat assessment: past twelve months (Asia Pacific)

Europe, Middle East and Africa: past twelve months

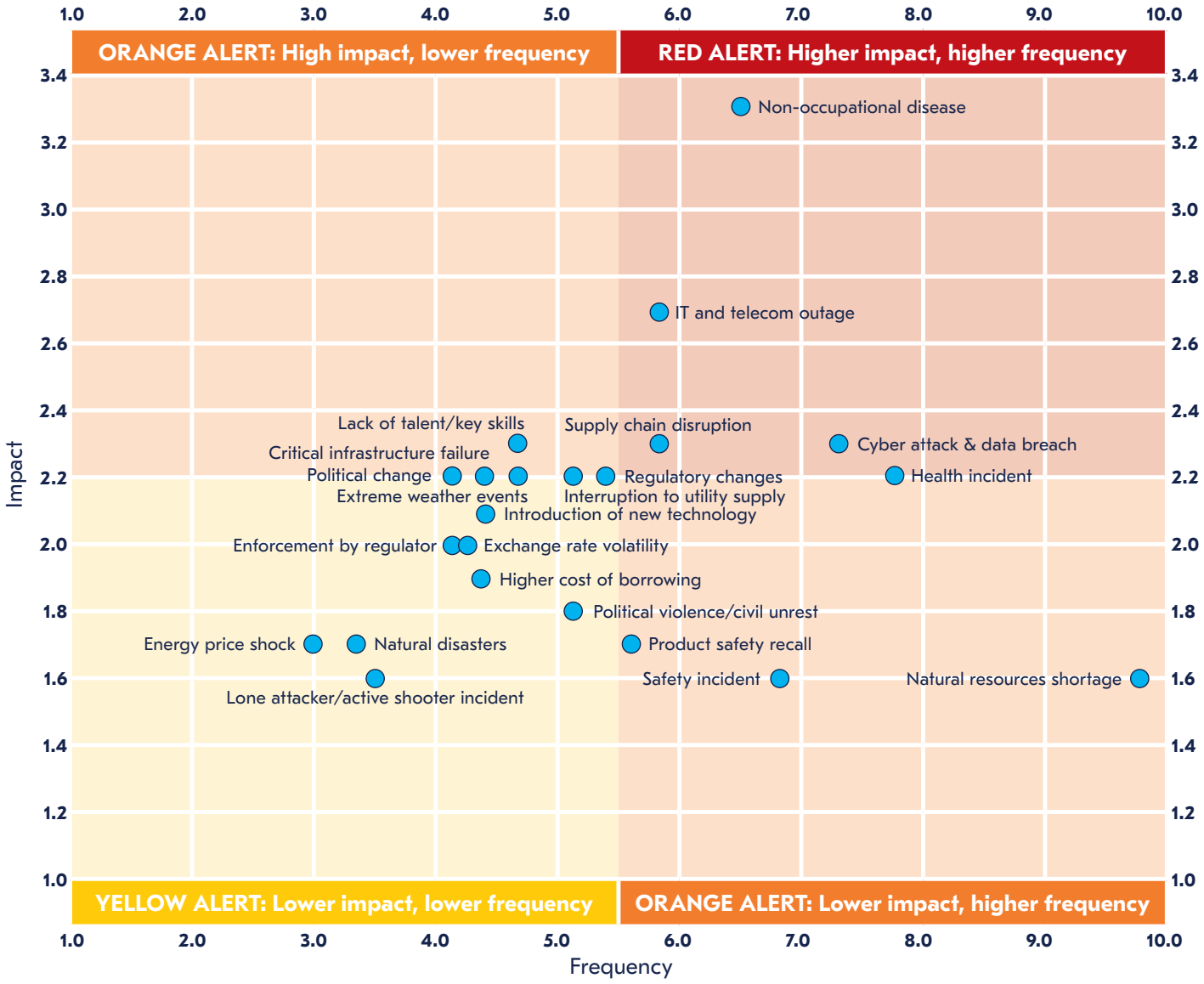


Figure 22. Risk and threat assessment: past twelve months (Europe, Middle East and Africa)

Americas: past twelve months

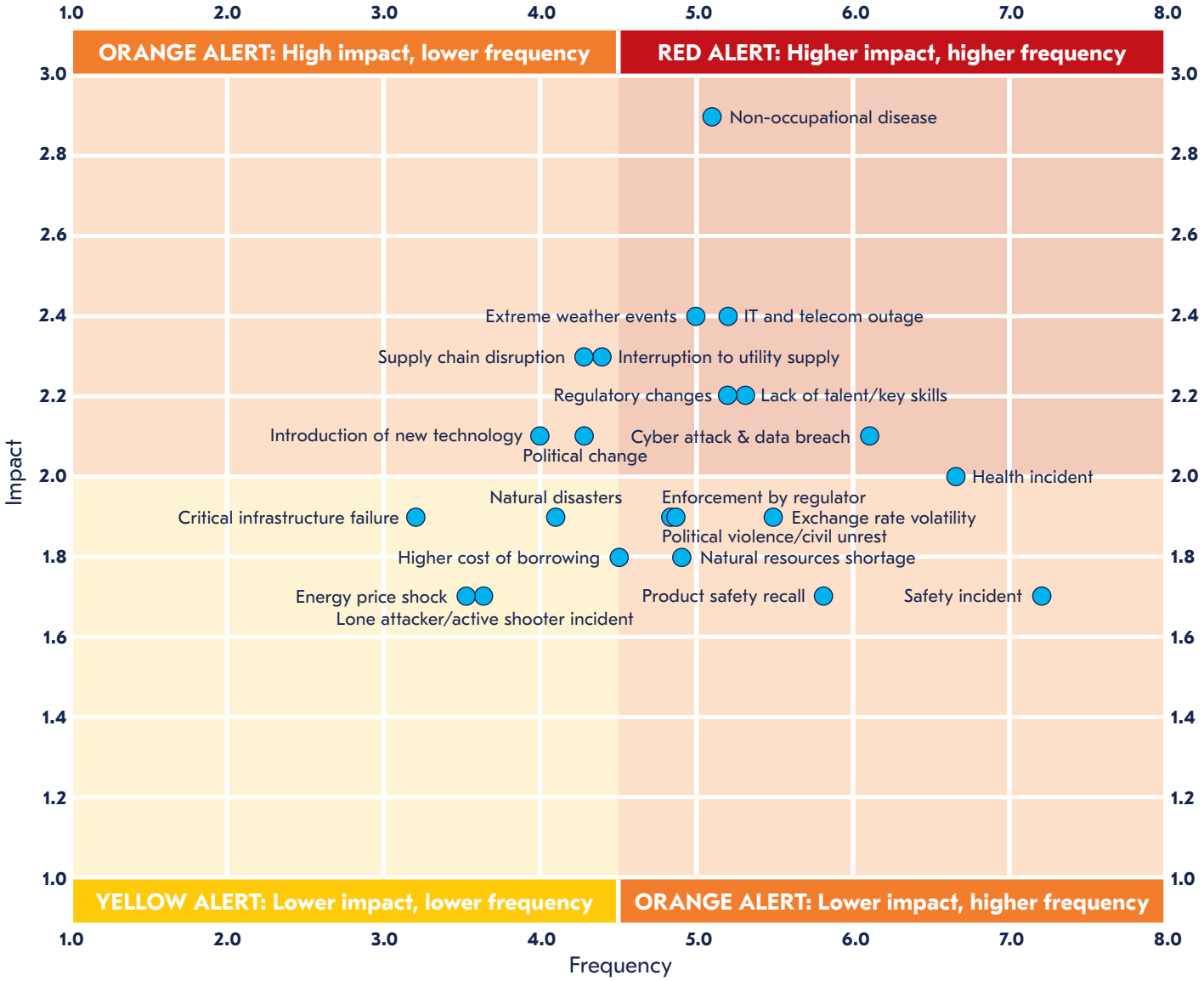


Figure 23. Risk and threat assessment: past twelve months (Americas)

Asia Pacific: next twelve months

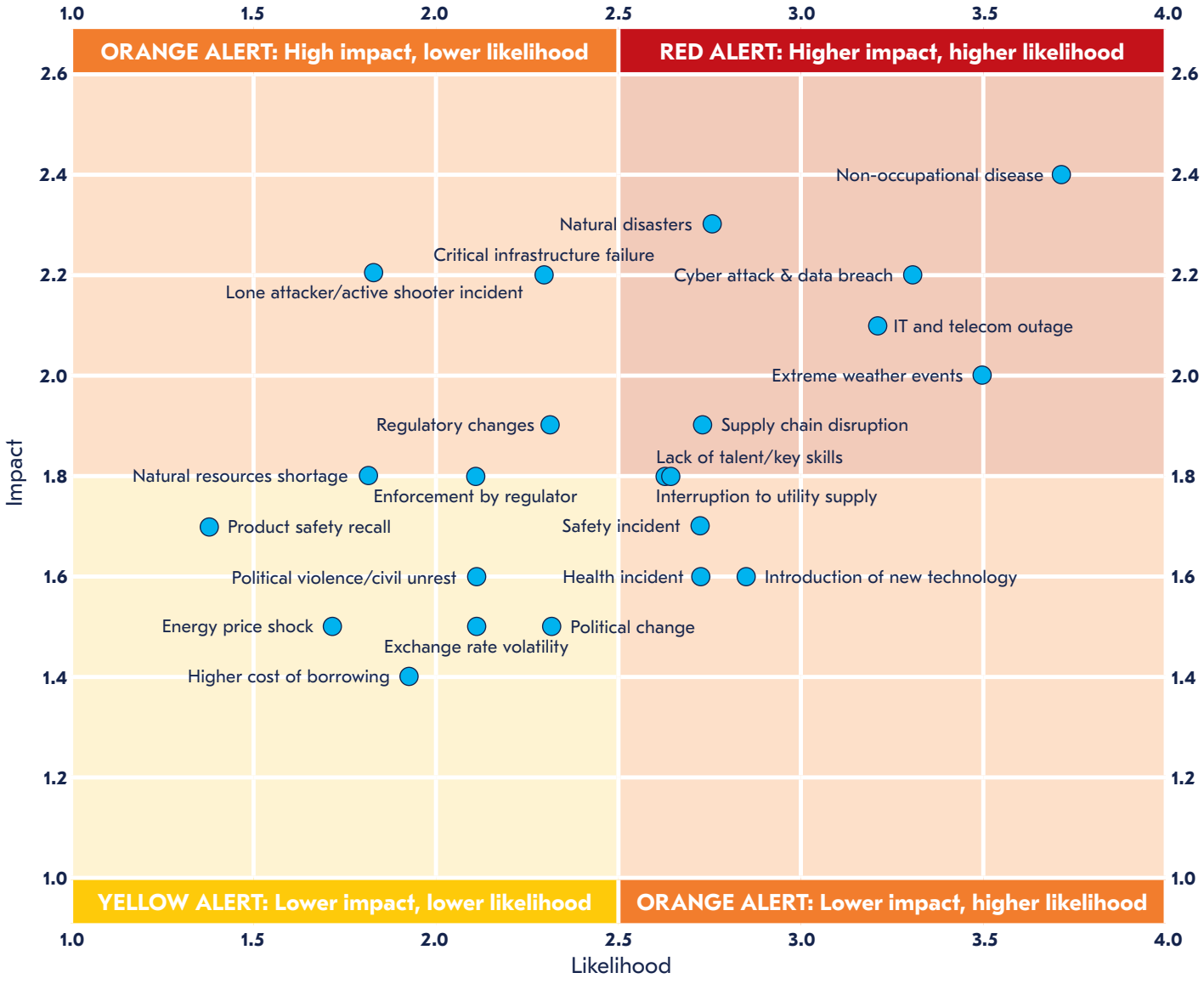


Figure 24. Risk and threat assessment: next twelve months (Asia Pacific)

Europe, Middle East and Africa: next twelve months

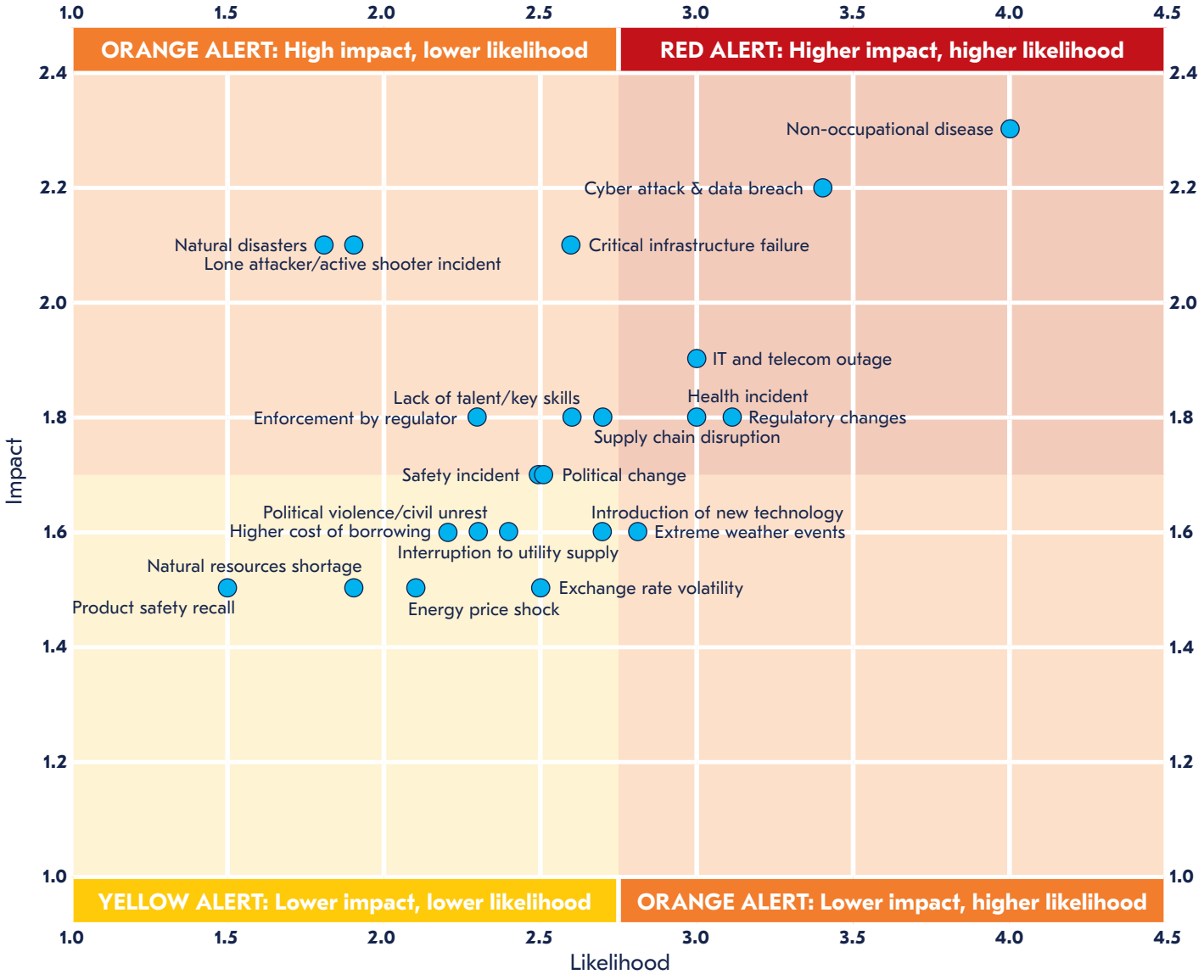


Figure 25. Risk and threat assessment: next twelve months (Europe, Middle East and Africa)

Americas: next twelve months

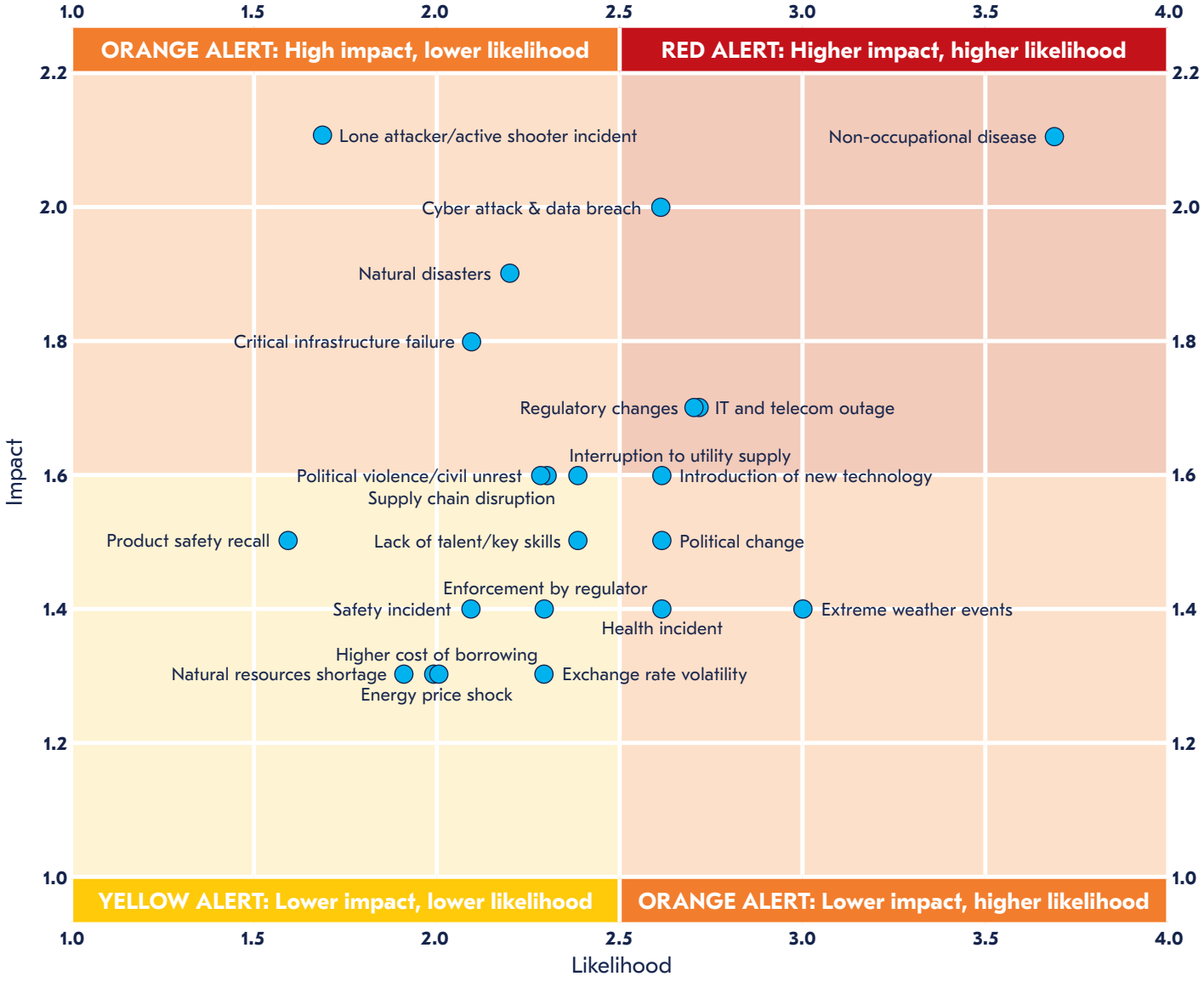


Figure 26. Risk and threat assessment: next twelve months (Americas)

About the Author

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**

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, 'inspiring trust for a more resilient world'. For over a century BSI has driven best practice in organizations around the world. Working with 84,000 clients across 195 countries, it is a truly global business with skills and experience across all sectors including automotive, aerospace, built environment, food and retail and healthcare. Through its expertise in Standards and Knowledge Solutions, Assurance Services, Regulatory Services and Consulting Services, BSI helps clients to improve their performance, grow sustainably, manage risk and ultimately become more resilient.

Visit: bsigroup.com

Correct as of March 2021

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